TRANSCEND

Transdisciplinary methods for societal impact assessment and impact creation for security research technologies

D4.1 – Plan for Dissemination and Communication

[WP4 – Create impact: disseminate, communicate and exploit results]

Funded by the European Union

Funded by the European Union. UK participants in Horizon Europe Project TRANSCEND are supported by UKRI grant number 10041916 (Trilateral Research). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or UKRI. Neither the European Union nor the granting authority nor UKRI can be held responsible for them.

Lead contributor	Elodie Reuge, Giacomo Bianchi, Guillaume Brumter; EOS
	Elodie.reuge@eos-eu.com, Giacomo.bianchi@eos-eu.com, Guillaume.brumter@eos-eu.com
Other contributors	Leanne Cochrane, Corinna Pannofino; TRI UK/ TRI IE (reviewers)
	Bamba Niang, Ilyana Skalli; Efus (peer reviewers)
	Lorin Camargo, Mar Marin; FMP (peer reviewers)

Due date	31.03.2023
Delivery date	31.03.2023
Type	Report
Dissemination level	PU=Public

Keywords	Dissemination, Communication, stakeholders, key messages, social media, website, target groups

Abstract

TRANSCEND aims to improve practices of citizen and societal engagement in security R&I. The action will contribute to the uptake of effective methods for citizen and societal engagement throughout the EU, so that civil society are given a louder voice, a place at the right tables and security practitioners are motivated and equipped to enhance such participation. To that end, TRANSCEND will develop a Toolbox of methods to enhance the involvement of civil society in security R&I. Additionally, the TRANSCEND Framework will present guidelines on how to design and structure meaningful civil society and public engagement for societal impact assessment for security research technologies and present domain-specific instructions for the use of the TRANSCEND toolbox.

These goals required the TRANSCEND Consortium to be committed to build up the TRANSCEND Network and reach out the general public as well as researchers, solutions providers, end-users and public authority, in order to effectively gather inputs, raise public awareness over the topic and disseminate the project outputs.

Therefore, the following Communication and Dissemination Plan was designed with the aim to firstly define the objectives, secondly identify the relevant audiences and their needs, and thirdly develop a consistent tailored method to engage the different stakeholders.

For this purpose, the Consortium partners based the Communication and Dissemination Plan on a multi-dimensional approach integrating the targeted audience profiles, the activities undertaken, such as the WP and pilots and the level of engagement. This approach resulted in key messages targeting specific stakeholders and focusing on specific tasks carried by the consortium partners.

Finally, this deliverable also presents the tools, platforms and profiles supporting the strategy both internally and externally. As such, Social Media accounts were created, the project website designed and the content to be shared defined with a particular focus on BlogSpot, articles and newsletter.

The following strategy and the set of measures and actions will support TRANSCEND in engaging with relevant stakeholders and achieving the goals set out in the Grant Agreement.

Revision Procedure

Version	Date	Description	Reason for Change	Author(s)
V0.1	17/02/2023	First Draft	-	EOS
V0.1	03.03.2023	Comments		TRI
V0.2	10.03.2023	Second Draft sent to peer reviewers (EFUS and FMP)		EOS
V0.3	17.03.2023	Feedback from the peer reviewers sent to EOS		EFUS and FMP
V0.4	22.03.2023	Third draft sent by EOS		EOS
V0.5	28.03.2023	Fourth draft sent by TRI		TRI
V0.6	28.03.2023	Fifth draft		EOS

Contents

1 Introduction 11
2 Engaging with the security ecosystem 12
2.1 Objectives for engaging 12
2.1.1 General objectives for engaging 12
2.1.2 Specific objectives for engaging with the European security ecosystem 12
2.2 Level of engagement 12
3 Stakeholder engagement 15
3.1 Identification of stakeholder groups and needs 15
3.1.1 Civil Society Organisations 15
3.1.2 Security Research Policy Makers 17
3.1.3 Impact Assessment Organisations 18
3.1.4 Security Practitioners 20
3.1.5 Security Solution Providers 21
3.1.6 Security Research Projects with similar activities 22
3.1.7 Research Community Experts 25
3.1.8 General Public and Media 26
3.2 Prioritisation of Groups 26
3.2.1 Priority Groups 27
3.2.2 Mid-Priority Groups 29
3.2.3 Other Groups 30
4 Key messages 31
4.1 General Rules 31
4.2 Key messages per objective and Stakeholder group 32
5 Dissemination and Communication Plan for engagement 38
5.1 Timeline 38
5.2 Dissemination plan: main means 39
5.2.1 Online dissemination means 39
5.2.2 Offline dissemination means 39
5.2.3 Dissemination through events 40
5.2.4 Synergies with other relevant projects 41
5.3 Communication plan: main means 41
5.3.1 Visual Materials 41

5.3.2 TRANSCEND Website 42
5.3.3 TRANSCEND Social media strategy 42
5.3.4 Newsletter 44
5.4 TRANSCEND Visual Identity and Social Media Communication Guidelines 45
5.5 TRANSCEND Crisis Communication Plan 45
6 Monitoring and Evaluation 46
7 Annexes 47
7.1 Annex 1 - TRANSCEND partners' social media accounts 47
7.2 Annex 2 - TRANSCEND Logo and colour Palette 47
7.3 Annex 3 – TRANSCEND Templates 48
7.4 Annex 4 – List of relevant events to attend 50
7.5 Annex 5 – Visual Identity and Social Media Guidelines 52
7.6 Annex 6 – Crisis Communication Plan 66
7.7 Annex 7 - Dissemination log 71
7.8 Annex 8 – Dissemination monitoring spreadsheet 73

Executive summary

By describing the basis of the dissemination and communication activities, the Plan for Dissemination and Communication (D4.1) creates the overall engagement approach that TRANSCEND will follow and respect during the project implementation, keeping an eye on the key pillars to be added to D4.1:

- Integrating the project into the EU and Global Security ecosystem;
- Providing reports and insights to the funding authority;
- Engaging with relevant stakeholders in the scope of the project's innovation support and validation services; and
- Disseminating value-added outputs to the relevant stakeholders.

To that purpose, the objectives were firstly defined as well as the expected impact and level of engagement to reach these goals. Secondly, the Plan for Communication and Dissemination needs to identify the targeted audience. In order to maximise the impact of the dissemination and communication activities, the audience was divided into target groups and their needs were defined. Such approach, building on the previous work consisting of defining suitable stakeholders for the TRANSCEND Network, enables the effective awareness campaign and involvement of key stakeholder needed for the success of the action.

Moreover, Communication and Dissemination should not take into consideration a tailored approach only, as mentioned above, to be successful. Indeed, key messages have been developed in order to determine the content to be communicated per Work Package and target group. This way, the right message will be shared to the right audience at the right moment.

Finally, the Communication materials, visual identity and vector of communication such as social media have been designed and produced to support the above-mentioned strategy to ensure the TRANSCEND project is recognizable by the target audience.

List of Tables

Table 1: List of acronyms/abbreviations 10
Table 2: Level of engagement 14
Table 3: List of Civil Society Organisations (retrieved from D2.1) 16
Table 4: List of Security Research Policy Makers (retrieved form D2.1) .. 17
Table 5: List of Impact Assessment Organisations (retrieved from D2.1) 19
Table 6: List of Security Practitioners (retrieved from D2.1) 20
Table 7: List of Security Solutions Providers (retrieved from D2.1) 22
Table 8: List of Security Research Projects with similar activities (retrieved from D2.1) 24
Table 9: List of Research Community Experts (retrieved from D2.1) 25
Table 10: Action Plan for High-Priority Target Groups 29
Table 11: Action Plan for Mid-Priority Groups 30
Table 12: Action Plan for Other Groups 30
Table 13: Key messages - WP1 34
Table 14: Key messages - WP2 35
Table 15: Key messages - WP3 36
Table 16: Key messages - WP4 37
Table 17 – KPIS 46
Table 18: TRANSCEND partners' social media accounts 47
Table 19: List of relevant event to attend (tentative) 51
Table 20: Metrics for the TRANSCEND Website 71
Table 21: Metrics for the Workshops 71
Table 22: Metrics for the Social Media 72
Table 23: Metrics for the Publications 72
Table 24: Metrics for the Newsletter 72
Table 25: Template Dissemination activities retrieved from the monitoring spreadsheet 74
Table 26: Template Communication Activities retrieved from the monitoring spreadsheet 74
Table 27: Template Media coverage retrieved from the monitoring spreadsheet 75
Table 28 Template from Publications retrieved from the monitoring spreadsheet 76

List of Figures

Figure 1: 1st TRANSCEND Factsheet 42
Figure 2: Screenshot TRANSCEND LinkedIn account..... 43
Figure 3: Screenshot TRANSCEND Twitter Account..... 44
Figure 4: TRANSCEND High Resolution Logo..... 47
Figure 5: TRANSCEND Colour Palette 48
Figure 6: Screenshot TRANSCEND Deliverable Template..... 49
Figure 7: Screenshot TRANSCEND PPT Presentation Template 50
Figure 8: Visual identity and social media guidelines 65
Figure 9: Screenshot of the TRANSCEND Crisis Communication Plan 70
Figure 10: Guideline for Communications and Dissemination Activities and Publications (extracted from the AGA and Horizon Programme Guidelines) 74

List of acronyms/abbreviations

Abbreviation	Explanation
BM	Border Management
CA	Consortium Agreement
CMINE	Crisis Management Innovation Network Europe
CS	Cyber Security
CSO	Civil Society Organisation
DoA	Description of Action
D	Deliverable
DC	Dissemination and Communication
DCNA	Disaster Competency Network Austria
DRS	Disaster Resilient Society
EC	European Commission
EDRI	European Digital Rights
ENISA	European Union Agency for Cybersecurity
ENLETS	Disaster Competency Network Austria
EOS	European Organisation for Security
EPTA	European Parliamentary Technology Assessment
EU	European Union
EU-LISA	The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
EUISS	The European Union Institute for Security Studies
EUROPOL	The European Union Agency for Law Enforcement Cooperation
FCT	Fighting Crime and Terrorism
FP7	Framework Programme 7
FRA	European Union Agency for Fundamental Rights
GA	Grant Agreement

Abbreviation	Explanation
IAIA	International Association for Impact Assessment
IAP	International Association of Public Participation
JRC	Joint Research Centre
LEA	Law Enforcement Agency
M	Month
NASK	National Research Institute
NCTV	Dutch National Coordinator for Counterterrorism and Security
NOYB	European Center for Digital Rights
OBFV	Austrian Federal Fire Fighter Association
PC	Project Coordinator
SMEs	Small and Medium Enterprises
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
THW	Technisches Hilfswerk
TRI	Trilateral Research
WP	Work Packages
WRR	The Netherlands Scientific Council for Government Policy

Table 1: List of acronyms/abbreviations

1 Introduction

The TRANSCEND plan for Communication and Dissemination is critical to enable and deliver on the TRANSCEND project ambitions and share in a meaningful and accessible manner the project's findings. This deliverable details the methodology and tools to be used during the project life-cycle to achieve the communication and dissemination objectives defined at the proposal stage.

The Dissemination and Communication Plan details the methodology and means for engaging the security ecosystem and general public and defines both general and specific objectives to ensure the efficacy of the outreach strategy.

The plan focuses on two main objectives:

- TRANSCEND's communication objectives: communication activities are the key enabler to effectively raise awareness about the main project's outcomes aimed at specific and predefined target groups. These activities should foster synergies with other projects and groups and should use TRANSCEND as a valid source of information.

- TRANSCEND's dissemination objectives: disseminating activities will focus on generating scientific knowledge based on valid and robust information sources. The project's findings should reach out to the maximum audience through the diffusion of knowledge, methodologies and procedures to deliver on the project's objectives.

Firstly, the vision of stakeholders' engagement and the objectives to be achieved will be defined (Section 2). Secondly, relevant stakeholders as well as their relations will be identified and defined through their needs in order to achieve the TRANSCEND objectives set in Section 2 (Section 3).

These groups will be then differentiated based on the TRANSCEND Network, which aims at actively involve various stakeholders. These stakeholders will represent the priority group for dissemination and communication activities. Tailored approaches and contents, through key messages, are present to maximize the impact of the Communication and Dissemination activities (Section 4).

Finally, the present deliverable also presents the foreseen project Communication and Dissemination activities with a timeline and the I channels, such as social media and website (Section 5). In appendices, the unique visual identity, materials and templates made for the purpose of external communication and dissemination are presented.

2 Engaging with the security ecosystem

2.1 Objectives for engaging

Developing a clear and straightforward approach behind the stakeholder engagement is crucial to establish a well-defined and structured engagement strategy. In this section, the general vision of the engagement strategy will be presented first (2.1.1), followed by a more specific and relevant reflection tailored for TRANSCEND (2.1.2).

2.1.1 General objectives for engaging

The general objectives for engaging are listed below:

- Reinforcing TRANSCEND's reputation: communicating about TRANSCEND will help to gain relevant stakeholders' trust;
- Promoting awareness with regards to TRANSCEND's outputs;
- Collecting relevant ideas: relevant targeted stakeholders will provide insights and contribute to enhance TRANSCEND's impact;
- Deepening TRANSCEND's impact: customized communication towards targeted stakeholders will support the uptake of the TRANSCEND's outputs.

2.1.2 Specific objectives for engaging with the European security ecosystem

"A genuine and effective Security Union must be the common endeavour of all parts of society. Governments, law enforcement, the private sector, education and citizens themselves need to be engaged, equipped, and properly connected to build preparedness and resilience for all, particularly the most vulnerable, victims and witnesses." [1]

The European security ecosystem is a broad, sensitive and complex sector, involving many types of organisations and activities. As clearly stated in the EU Security Strategy, a lot of different stakeholders need to be part of building it. The identification and involvement of the relevant targeted stakeholders will ensure that the TRANSCEND's results are targeted to their needs and concerns.

2.2 Level of engagement

Like many EU funded projects, TRANSCEND will follow the spectrum of public participation developed by the International Association of Public

[1] Communication from the commission to the European Parliament, the European Council, the council, the European economic and social committee and the committee of the regions on the EU Security Union Strategy from the 24.07.2020 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&rid=6

Participation (IAP[2]), including five levels of engagement: 1) informing, 2) consulting, 3) involving, 4) collaborating and 5) empowering. The table below summarises the chosen approach within TRANSCEND:

	Informing	Consulting	Involving	Collaborating	Empowering
Public Participation objectives	Provide the public with relevant and constructive information, the purpose being the public to understand the goals of the project and the concept of Resilient Infrastructure	Get the public's feedback on decisions taken within TRANSCEND	Ensure that the public concerns and aspirations regarding TRANSCEND are well-received and taken into consideration by the consortium	Partnership built with the public in several aspects of TRANSCEND	Place decision making in the hand of the Public

[2] "IAP2 is the preeminent international organization advancing the practice of public participation. Our mission is to advance and extend the practice of public participation through professional development, certification, standards of practice, core values, advocacy and key initiatives with strategic partners around the world." https://www.iap2.org/page/about, consulted on the 27th of January 2023

	Informing	Consulting	Involving	Collaborating	Empowering
Promises made to the Public	Keep the public informed about the outcomes of TRANSCEND	Keep the public informed, of its concerns and provide feedback on how its input influenced a decision taken within TRANSCEND	Make sure that its concerns are reflected in the alternatives developed and provide feedback on how its input influenced the decision taken	Work closely with the public in incorporating its advice and recommendations into the decisions	Implement what the public decides within and through TRANSCEND

Table 2: Level of engagement

3 Stakeholder engagement

3.1 Identification of stakeholder groups and needs

This section presents the stakeholders' profiles based on the outputs of D2.*1 Landscape of security research: CSO Mapping, Strategies and Best Practices for Citizen and Societal Engagement*. The project seeks to create the TRANSCEND Network (WP2, *Stakeholder mapping, networking, mutual learning and training to enhance citizen and societal engagement*) which will include a wide array of stakeholders, from Law Enforcement Agencies to Civil Society Organisations. Therefore, identifying and understanding the stakeholders' profiles is crucial to involve the relevant partners, raise awareness on the project and disseminate its outputs.

To that end, the partners contributing to WP4 have identified eight (8) groups of stakeholders to reach out to. These groups are presented below with a tentative list of entities or organisations, at national, European and international levels, to be targeted throughout and after the project life cycle. Moreover, the needs as well as the impact from both the consortium and stakeholders' perspectives are presented to ensure the efficiency of the Communication and Dissemination activities and successfully achieve the project's objectives.

3.1.1 Civil Society Organisations

Targeted Audience:

Civil Society Organisations are interest groups serving the general interest of the society. CSOs are non-profit, non-governmental and important stakeholders in the dialogues between Policy Makers and civilians, as stated in Art. 15 of the TFEU and Art. 11 of TEU.

Based on the outputs from the SecurePART Project (FP7, GA n 608039) CSOs have different profiles and models and have been increasingly involved in European security research.

A preliminary list of CSOs is presented in the table below.

International Level	
	Statewatch
	Transnational Institute
	Human Rights House Foundation
EU Level	
	European Digital Rights (EDRi)

	Yes we Hack
	NOYB – European Center for Digital Rights
National Level	
Belgium	Open Knowledge Belgium
Bulgaria	Law and Internet Foundation
Czech Republic	Česko Digital
Germany	Freiheit statt Angst
Spain	Political Watch
Kosovo	Open Data Kosovo
Hungary	Code for Hungary
The Netherland	Waag
Poland	Panoptykon

Table 3: List of Civil Society Organisations (retrieved from D2.1)

Audience needs:

CSOs are critical to achieve the TRANSCEND objectives as being the key stakeholders providing feedback and experience on their role in the development of innovative technological solutions for the security sector. CSOs could benefit from both the participation in and the outputs from the TRANSCEND project.

Even though the SecurePART Project has underlined the increased involvement of CSOs in developing innovative solutions in the security domain, CSOs still face barriers to their involvement in the design of innovative solutions. Indeed, the SecurePART project stressed the lack of access to security research actions and the lack of visibility from security actors. The industry sector or researchers may also be reluctant to engage CSOs due to confidentiality and commercial concerns[3].

Given the above-mentioned barriers, CSOs could benefit from a rare opportunity to participate in the design of the TRANSCEND framework, which will strengthen their participation and foster their active participation in security research. Moreover, CSOs will contribute to the pilots. For this purpose, the mapping of CSOs (Task 2.1) considers different profiles at the international, European and National levels.

TRANSCEND Impact:

[3] SecurePART Project results, consulted on the 10/03/2023, https://cordis.europa.eu/project/id/608039/reporting

The CSOs' involvement in the TRANSCEND project will also be a condition for its success. The access to CSO inputs, methodologies and experiences will assist the consortium in designing appropriate tools to enhance the involvement and effectiveness of their cooperation with both policy makers and industries.

Moreover, CSOs will be involved during the testing phases on the four security domains explored in the TRANSCEND project (DRS, CS, BM and FCT). For this reason, a set of different CSOs, involved in specific security domains and at different levels (European, international and national levels) is selected to better emphasize the security landscape.

3.1.2 Security Research Policy Makers

Targeted Audience:

Security Research Policy Makers include organisations, experts, and policy makers working in at least one of the four security domains identified (DRS, CS, FCT, BM) and involved in the design of either the appropriate Framework Programmes or the Regulatory Framework for the development of innovative solutions for the security sector. The Security Research Policy Makers set priorities through the identification of needs and the evaluation of threats.

A list of tentative organisations and institution is presented below:

EU Level	
European Institutions	European Commission (DG HOME)
European Parliament	European Parliament (Industry, Research and Energy Committee)
	European Parliament (Civil Liberties, Justice and Home Affairs Committee)
	European Parliament (Artificial Intelligence in a Digital Age Committee)
European Agencies	EUROPOL
	ENISA
	EUISS
	Eu-LISA
National Level	
Poland	NASK (National Research Institute)

Table 4: List of Security Research Policy Makers (retrieved form D2.1)

Audience Needs:

The community of Security Research Policy Makers would use the TRANSCEND project's outputs, the toolbox, frameworks and overall findings, in the context of its responsibilities regarding their procurements procedures, call for tender design and cooperation with civil society.

Considering the various nature, at the European and National levels, of these organisations, their respective framework for involving civil society differ depending on various aspects, such as their competences and focus. The TRANSCEND project aims at providing a robust framework to ease and improve the involvement in the innovative security solutions' design and deployment phases.

Through their responsibilities, Security Research Policy Makers have the opportunity to foster better or more efficient cooperation between Civil Society and the industries and researchers.

TRANSCEND Impact:

The Security Research Policy Makers will support and contribute to the TRANSCEND project by sharing their experience as a mediator between the industries and Civil Society. Policy Makers already base the Framework Programmes and other orientation documents on the outputs of public consultations where public, private and civil organisations can participate.

The TRANSCEND consortium will engage with Policy Makers to better identify their needs. Moreover, the above-mentioned Public Authorities will strengthen the reliability of the policy briefs to be produced for each pilot areas and their reach. Finally, the TRANSCEND project will also deliver four implementation support workshops, specifically designed for Policy Makers, in order to ensure their proper involvement in the design and their understanding of the TRANSCEND Toolbox and other project outputs.

3.1.3 Impact Assessment Organisations

Targeted Audience:

Impact Assessment Organisations advise and support public and private organisations on the impact of their projects, operations or strategies. The TRANSCEND project focuses on the Impact Assessment Organisations involved in security research, and especially in the four security areas of the project.

The table below presents a tentative list of Impact Assessment Organisations:

EU level	
	European Technology Assessment Group
European Parliament	European Parliamentary Technology Assessment (EPTA)
European Agency	European Union Agency for Fundamental Rights (FRA)
Council of Europe	Council of Europe and Artificial Intelligence
European Commission	Joint Research Centre
International Level	
International Association	International Association for Impact Assessment (IAIA)
National Level	
Austria	Austrian Society for Disaster Risk Reduction

Table 5: List of Impact Assessment Organisations (retrieved from D2.1)

Audience Needs:

The Impact Assessment Organisations could use the TRANSCEND project's outputs as a comprehensive methodology, consisting of the TRANSCEND Toolbox and Framework, to better involve Civil Society in its impact assessment. Indeed, even though impact assessment, either ex-ante or ex-post, are common, their accuracy can be harmed due to the lack of responses and the insufficient number of key stakeholders involved. They may also observe and contribute to the pilots to be organised for the four security areas.

TRANSCEND Impact:

The TRANSCEND consortium is willing to engage with Impact Assessment Organizations to benefit from their experience as regard to their impact assessment methodologies and identify the gaps and needs in order to increase the civil society perspective in the assessment. For this purpose, the TRANSCEND consortium needs to understand the threshold for positive and negative impacts as well as the methodologies to correct, mitigate or strengthen a specific effect. Impact Assessment Organizations will be invited to join the TRANSCEND Network, having access to the consortium Members and project's design and outputs.

3.1.4 Security Practitioners

Targeted Audience:

Security practitioners are public entities enforcing the law and the other entities supporting them in the implementation of their competencies. In the context of the Communication and Dissemination plan, the differentiation is made between the terms Security Practitioners and Security Providers. The Security Practitioners are direct public security professionals and Law Enforcement Agencies, having a competence in the fields of intelligence, threats, risks and vulnerabilities. The term of Security Providers refers to industrials, large companies, SMEs and Research Organisations, providing solutions to the first category and will be further developed in the next sub-section. Indeed, such differentiation is important considering their different characteristics, needs and behaviour regarding, on the one hand, the private for profit and on the other hand their public responsibility nature.

The tentative list below presents Ministries, LEAs and other actors involved in Public Safety and Protection:

EU Level	
	European Network of Law Enforcement Technology Services (ENLETS)
	EU LEAs
	EU Medical and Disaster Relief Orgs
National level	
The Netherlands	Dutch National Cybersecurity Centre
	Dutch Police
	Dutch National Coordinator for Counterterrorism and Security (NCTV)
	Dutch Immigration & Naturalisation Service
Belgium	Belgian Crisis Center
	Belgian Red Cross
France	Sapeurs Pompiers de Paris
	Direction Générale de la Gendarmerie Nationale, Service de la Transformation
Germany	Technisches Hilfswerk (THW)
Austria	Austrian Federal Ministry of Interior
	Austrian Federal Fire Fighter Association (ÖBFV)

Table 6: List of Security Practitioners (retrieved from D2.1)

Audience Needs:

Over the past, some technologies were used by LEAs and other internal security authorities to address specific circumstances, such as the mobile application for contact tracing in the context for the COVID-19 pandemic or during the emergency states following the terror attacks across Europe in 2015 and later. The Civil Society has raised doubts over these technologies respecting their fundamental and individual rights.

Consequently, the Security Practitioners could benefit from the TRANSCEND project to better involve the Civil Society in the implementation of innovative solutions to make the European society safer. Indeed, the TRANSCEND Toolbox and Framework will give effective ways of involving and cooperating with Civil Society as citizens are the first beneficiaries of a safer environment.

TRANSCEND Impact:

The Security Practitioners will support the TRANSCEND consortium in identifying the existent framework for cooperation with Civil Society, as well as the barriers and limitations to its implementation. They will also contribute to the better understanding of opportunities offered by new technologies for security practitioners.

To that end, TRANSCEND will reach out the Security Practitioners and invite them to be part of the TRANSCEND Network, which will organise the TRANSCEND Framework Summit and set up workshops and pilot tests in the field of expertise. Existing Security Practitioners will also be contacted using the experience of consortium Members.

3.1.5 Security Solution Providers

Targeted Audience:

As mentioned in Section 3.1.4, Security providers are private entities – companies, SMEs, and Research Organisations- providing Security Practitioners with innovative solutions necessary to the implementation and conduct of their missions and authorities. Security Providers develop these solutions based on the Security Practitioners needs, capacities and capabilities.

The TRANSCEND project will benefit from its link to the Security Solution providers involved in the development of various technologies in the areas of interest through the members of its consortium.

The table below presents a tentative list of Security Providers:

Sector	Audience
Border Management	Airbus
	IDEMIA
Cybersecurity	Conceptivity
	LAUREA
FCT	SYNYO
	KEMEA
DRS	Satways

Table 7: List of Security Solutions Providers (retrieved from D2.1)

Audience Needs:

As mentioned above, the Security Practitioners develop sensible solutions that may raise fear and suspicions from Civil Society. Security Providers usually consider the compliance with the legal framework only. Therefore, they need to better understand the processes leading to this lack of trust and establish methodologies to address them.

TRANSCEND Impact:

Security Providers could use the TRANSCEND Framework and Toolbox to design innovative solutions accepted by Civil Society. This approach will enable the Security Providers to propose to procurement authorities operational solutions which will have ethical and societal benefits.

Security Providers will contribute to the improved understanding of internal development processes involved in the innovation life cycle in the field of security. Security providers will be directly involved through the TRANSCEND Framework and can share their needs, views and ambitions through a survey. They will also benefit from the project's outputs and especially the workshops and test pilots.

3.1.6 Security Research Projects with similar activities

Targeted Audience:

Security research projects with similar activities refers to EU-funded projects in the field of security in one or more of the focus areas (CB, DRS, BM and FCT) which involved, among others, Networks of Security Practitioners, researchers, innovators and Civil Society Organisations.

The table below presents a tentative list of EU projects with similar activities:

Internal Security Fund		
ISF - Police	PACTESUR	Protect Allied Cities against TErrorism in Securing Urban aReas
	SECU4ALL	Training local authorities to provide citizens with a safe urban environment by reducing the terrorist attacks related risks in public spaces
	SHIELD	SolutionS to enHance Interfaith protEction of pLaces of worship from terrorist Danger
	CYBERSPACE	
7th Framework Programme for Research and Innovation		
FP7-SEC-2013-1	DRIVER +	Driving Innovation in Crisis Management for European Resilience
Horizon 2020		
H2020-SESAR-2016-1	IMPETUS	Intelligent Management of Processes, Ethics and Technology for Urban Safety
H2020-BES-2015	PROTECT	
H2020-SU-SEC-2019	ICARUS	Innovative AppRoaches to Urban Security
H2020-SEC-2016-2017-2	CCI	Cutting Crime Impact
H2020-SU-SEC-2019	LINKS	Strengthening links between technologies and society for European disaster resilience
H2020-SU-SEC-2020	RISKPACC	Integrating Risk Perception and Action to enhance Civil protection-Citizen interaction
H2020-SEC-2016-2017-2	MEDEA	Mediterranean & Black Sea Security Practitioners' Network
H2020-SEC-2016-2017-1	DARENET	Danube River Region Practitioners Network
H2020-SEC-2016-2017-1	FIRE-IN	EU-wide collaborative platform for First Responders, researchers and industries
H2020-SEC-2016-2017-1	ENCIRCLE	European CBRN Innovation for the Market Cluster

H2020-SEC-2016-2017-2	NO-FEAR	Network Of practitioners For Emergency medicAl systems and cRitical care
H2020-ICT-2017-1	Procure2Innovative	European Network of Competence Centres for Innovation Procurement
H2020-SEC-2016-2017-1	i-LEAD	Innovation - Law Enforcement Agencies Dialogue
H2020-SEC-2016-2017-1	ILEANET	Innovation by Law Enforcement Agencies networking
H2020-SU-SEC-2020	CYCLOPES	Cybercrime Law Enforcement Practitioners' Network
H2020-SEC-2016-2017-2	PEN-CP	Pan-European Network of Customs Practitioners
H2020-SU-SEC-2019	CC-DRIVER	Understanding the drivers of cybercriminality, and new methods to prevent, investigate and mitigate cybercriminal behaviour A Research
H2020-SU-DS-2020	TRUSTaWARE	Enhancing Digital Security, Privacy and TRUST in softWARE
H2020-SU-SEC-2019	PANDEM-2	Pandemic Preparedness and Response
European Regional Development Fund		
NA	SURE	Smart Urban Security and Event Resilience
Others		
NA	RECHECK	Resilience check

Table 8: List of Security Research Projects with similar activities (retrieved from D2.1)

Audience Needs:

The running EU projects have similar needs to the TRANSCEND project in terms of scientific knowledge and inputs to develop robust methodologies and/or innovative solutions for Security Providers and Security Practitioners. Moreover, future and on-going projects need to enrich their outreach capacity through new networks and knowledge communities. They could use the findings and outputs of the TRANSCEND project in order to design civil society friendly solutions.

Furthermore, completed projects may also benefit from participating to the TRANSCEND Network as a facilitator to disseminate their outputs to a wider public, including CSO, and exploit their results based on civilians' perspectives.

TRANSCEND Impact:

Using the existing partners' networks, these projects will be targeted and approached to be part of the TRANSCEND Network. These stakeholders will also be invited to participate in the TRANSCEND events.

3.1.7 Research Community Experts

Targeted Audience:

The Research Community Experts summoned the organisations involving researchers and academics studying the field of civil society involvement and security, and more specifically, in the field of cybersecurity, civil protection, fight against crimes and border management.

The table below presents Research Community Experts:

Level	Name
Europe	CMINE – Crisis Management Innovation Network Europe
	JRC Competence Centre on Participatory and Deliberative Democracy
Austria	DCNA Disaster Competency Network Austria
Netherlands	The Netherlands Scientific Council for Government Policy (WRR)
United-Kingdom	University of Warwick

Table 9: List of Research Community Experts (retrieved from D2.1)

Audience Needs:

The Research Community Experts studying the security sector need networks to disseminate their findings and knowledge. They also need to validate such findings in real-case scenarios where all stakeholders are represented.

TRANSCEND Impact:

The Research Community could use TRANSCEND as means to test and validate their findings during the four testing phases. Moreover, Experts could enrich their knowledge using the outputs of such testing phases and benefit from the opportunity to work with all stakeholders, from Civil Society Organisations to Security Providers, as part of the TRANSCEND Network

and engage them directly during the various TRANSCEND meetings and events.

3.1.8 General Public and Media

Targeted Audience:

EU civilians and EU-wide media outlets (including but not limited to Politico EU, EUobserver, Euractiv).

Audience Needs:

In the context of the TRANSCEND project, civil society is a key stakeholder involved though Civil Society Organisations. However, civilians are not always structured. Even though innovation in the field of security is a societal challenge, citizens and members of the public raise their voice when such technologies harm their values and fundamental rights. Therefore, civilians need to be informed on initiatives.

TRANSCEND Impact:

The TRANSCEND project should communicate effectively to the widest audience and promote its findings and commitment to develop innovative solutions for security while promoting the European values and way of life. The project's aims, objectives, and outputs will be presented though various media, press releases and events.

3.2 Prioritisation of Groups

This section hierarchically classifies the targeted audiences into three groups: Priority, mid-priority and other groups. Each section presents the targeted audience in a table with the key actions to be implemented by the consortium as well as the means for the actions to be completed.

Such taxonomy of the audiences aims at achieving a key milestone of the TRANSCEND project: developing the TRANSCEND Network. Indeed, the TRANSCEND Network will be a key enabler for the purpose of the action. For this reason, the stakeholders identified as critical to gather inputs on the existing methodologies and processes to involve Civil Society are the prior target audience of the TRANSCEND Communication and Dissemination plan. They are therefore classified under the Priority Group. Other potential stakeholders that could bring additional knowledge relevant to the action are classified under the Mid-Priority and Other Categories. This approach refers to the level of engagement for each of them and does not refer to their importance as they should all benefit from TRANSCEND and could all contribute to its success.

3.2.1 Priority Groups

The Priority Groups include all stakeholders that will take part in the TRANSCEND Network and which are directly linked to the TRANSCEND action. Their involvement will be sustained throughout the project life cycle.

Stakeholder Group	Purpose	Key Actions	Means of Engagement
Civil Society Organisations	TRANSCEND Network	Gather inputs and solution validation	Website, newsletters, promotional material
			Workshops, trainings, mutual learning and pilots
		Promote uptake of project solutions and outputs	Policy briefs
			Press releases
			TRANSCEND Network, website and social media
Security Research Policy Makers	TRANSCEND Network	Promote uptake of project solutions and outputs	Policy oriented events
			Workshops
			Transcend Framework Summit
		Create liaisons with Policy Makers	Policy briefs
			Networks of practitioners events

Stakeholder Group	Purpose	Key Actions	Means of Engagement
			TRANSCEND Network, website and social media
Security Practitioners	TRANSCEND Network	Promote uptake of project solutions and outputs	Website, newsletters, promotional material
			Policy briefs
		Create liaisons with Policy Makers	Networks of practitioners events
			TRANSCEND Network, website and social media
Security Solution Providers	TRANSCEND Network	Gather inputs and solution validation	Website, newsletters, promotional materials
			Policy briefs
		Promote uptake of project solutions and outputs	Community, industry events
			TRANSCEND Network, website and social media
Security Research Projects with similar activities	TRANSCEND Network	Promote uptake of project solutions and outputs	Website, newsletters, promotional materials
			Networks and clusters of projects

Stakeholder Group	Purpose	Key Actions	Means of Engagement
		Create liaisons with EU-funded projects	TRANSCEND Network, website and social media
Research Community Experts	TRANSCEND Network	Gather inputs and solution validation	Networks and clusters of projects
		Promote uptake of project solutions and outputs	Participation to scientific articles
		Contribute to robust solution design	TRANSCEND Network, website and social media

Table 10: Action Plan for High-Priority Target Groups

3.2.2 Mid-Priority Groups

The category of Mid-priority Group includes stakeholders having also a potential important impact on the successful completion of the TRANSCEND project. The action may require additional inputs to be aggregated and for the purpose of the pilot phases. For this reason, the Project will, in an organised and frequent manner, engage with the following group.

Stakeholder Group	Purpose	Key Actions	Means of Engagement
Impact Assessment Organisations	TRANSCEND Network	Gather inputs and solution validation	Website, newsletters, promotional materials
		Promote uptake of project solutions and outputs	Community, industry events
		Contribute to robust solution design	TRANSCEND Network, website and social media

		Create liaisons with Policy Makers	

Table 11: Action Plan for Mid-Priority Groups

3.2.3 Other Groups

Finally, the TRANSCEND consortium will seize any opportunity to raise awareness on the action's outputs and let the below group contribute by providing inputs:

Stakeholder Group	Purpose	Key Actions	Means of Engagement
General Public and Media	TRANSCEND Network	Raise awareness on project outputs and other activities	Website, newsletters, promotional materials
			TRANSCEND Framework Summit
			Press releases
			TRANSCEND Network, website and social media

Table 12: Action Plan for Other Groups

4 Key messages

Developing, deploying and delivering appropriate and efficient messages for the stakeholders' engagement is one of the major cornerstones for a successful Communication and Dissemination strategy. Indeed, key messages are important as they play a crucial role in order to reach a satisfied and comprehensive communication and dissemination standard about the main points and highlights of a project. Those main points and highlights will be addressed and delivered to the variety of audiences previously presented and described in this document.

Key messages help to define the project, highlight TRANSCEND's achievements and impact, and convey the value of the project to a wider audience. By having clear, concise, and compelling key messages, the consortium can effectively communicate the importance and value of the project and help to generate support and interest in it.

In this section we focus more on the preliminary assessment and objectives of TRANSCEND, presenting the general rules, the high-level messages and the specific objectives of the project.

4.1 General Rules

Messages need to be adapted according to interest and have to be customized for each target audience, and even more for any relevant idea, activity or research outcome that the consortium wants to share. Not all messages can be fundamental, and they must have the following characteristics:

- Simple and positive
  Key messages should be short and to the point (direct and straightforward), concise, clear and written in a plain language that is easy to understand. They should highlight the achievements of the project and they should avoid using technical jargon or acronyms that may not be familiar to the audience.

- Focus on the key points
  Identify TRANSCEND's most important activities and outcomes and be able to highlight these. It should be a good practice to avoid including too many details.

- Tailored to the audience
  TRANSCEND will engage different audiences, who might be interested in different aspects of the project. Highlighting the most relevant aspects and points that will be most relevant and interesting to the targeted audience is crucial.

- Consistent

Key messages need to be delivered using a consistent tone. They must be aligned with the overall TRANSCEND goals and objectives.

- Coherent
  Key messages must always take into account TRANSCEND's objectives and peculiarities.

4.2 Key messages per objective and Stakeholder group

Developing and sharing concise, direct and straightforward key messages is a crucial action in order to achieve a successful communication and dissemination. Messages can be considered one of the main pillars of the actions and activities that TRANSCEND wants to communicate to the different audiences previously presented and described.

Key messages, as presented below, take in consideration the different aspects of the project, the number and features of stakeholders, or potential stakeholders, and they will be addressed, tailored and customised taking into account the different audience which they refer to.

In the tables below, key messages are presented as a reflection of the contents and scopes of the different TRANSCEND work packages, such as work packages 1, 2, 3 and 4.

Key messages have been designed based on three factors: (a) the objectives included in each Work Package (b) the target audiences (c) the added value of TRANSCEND for each targeted audience group.

WP1 – DEVELOP TRANSCEND TOOLBOX	Security Practitioners	Policy Makers	Research Organisations	Citizens/The public, NGOs, CSOs and Media	Other Relevant EC funded projects
OBJECTIVES	**KEY MESSAGES**				
To provide an overview of methods for citizen and societal engagement, notably of methods to involve citizens, in security R&I; including studies of which methods do (not) work in practice	In order to involve societal stakeholders and citizens, and to take into account ethical, human rights and societal aspects, TRANSCEND will use these to develop or deploy (new) technologies. Critically,	TRANSCEND will provide a set of methods to promote collaboration between security professionals, industry, academia, and CSOs / citizens. Critically, you can require them to follow these	TRANSCEND will provide a set of methods to contribute to the development and/or deployment of (new) technologies. Critically, these methods facilitate collaboration, e.g., with	TRANSCEND will provide a set of methods in order to contribute to the development and/or deployment of (new) technologies. Critically, these methods can empower you to collaborate	TRANSCEND will provide a set of methods in order to develop or deploy (new) technologies in your project, and to organize collaboration between: security professionals, industry, government,

WP1 – DEVELOP TRANSCEND TOOLBOX	Security Practitioners	Policy Makers	Research Organisations	Citizens/The public, NGOs, CSOs and Media	Other Relevant EC funded projects
	these methods facilitate collaboration, e.g., with industry, government, academia, and CSOs / citizens.	methods when you fund their projects.	security practitioners, industry, government, and CSOs / citizens.	with, e.g., security practitioners, industry, academia, and government.	academia, and CSOs / citizens (Quadruple Helix).
To provide an overview of methods for ethical, human rights and social impact assessment of security technologies, notably of methods for the early design phases; including studies of ways to prevent or mitigate negative outcomes, where possible	In order to involve societal stakeholders and citizens, and to take into account ethical, human rights and societal aspects, TRANSCEND will use these to develop or deploy (new) technologies. Critically, these methods facilitate collaboration, e.g., with industry, government, academia, and CSOs / citizens.	TRANSCEND will provide a set of methods to promote collaboration between security professionals, industry, academia, and CSOs / citizens. Critically, you can require them to follow these methods when you fund their projects.	TRANSCEND will provide a set of methods to contribute to the development and/or deployment of (new) technologies. Critically, these methods facilitate collaboration, e.g., with security practitioners, industry, government, and CSOs / citizens.	TRANSCEND will provide a set of methods in order to contribute to the development and/or deployment of (new) technologies. Critically, these methods can empower you to collaborate with, e.g., security practitioners, industry, academia, and government.	TRANSCEND will provide a set of methods in order to develop or deploy (new) technologies in your project, and to organize collaboration between security professionals, industry, government, academia, and CSOs / citizens (Quadruple Helix).
To develop a TRANSCEND Toolbox, a set of methods to involve citizens to test and deploy in pilots, and improve in an iterative process, learning from the pilot findings (D1.3 will summarize and present	In order to involve societal stakeholders and citizens, and to take into account ethical, human rights and societal aspects, TRANSCEND will use these to develop or deploy (new) technologies. Critically, these methods	TRANSCEND will provide a set of methods to promote collaboration between security professionals, industry, academia, and CSOs / citizens. Critically, you can require them to follow these methods when you	TRANSCEND will provide a set of methods to contribute to the development and/or deployment of (new) technologies. Critically, these methods facilitate collaboration, e.g., with security practitioners,	TRANSCEND will provide a set of methods in order to contribute to the development and/or deployment of (new) technologies. Critically, these methods can empower you to collaborate with, e.g., security	TRANSCEND will provide a set of methods in order to develop or deploy (new) technologies in your project, and to organize collaboration between: security professionals, industry, government, academia, and CSOs /

WP1 – DEVELOP TRANSCEND TOOLBOX	Security Practitioners	Policy Makers	Research Organisations	Citizens/The public, NGOs, CSOs and Media	Other Relevant EC funded projects
findings from all WP1: tasks 1.1, 1.2, 1.3 and 1.4)	facilitate collaboration, e.g., with industry, government, academia, and CSOs / citizens.	fund their projects.	industry, government, and CSOs / citizens.	practitioners, industry, academia, and government.	citizens (Quadruple Helix).
To develop a method to evaluate or measure citizen and societal engagement, which can be used in parallel to the TRANSCEND Toolbox	In order to involve societal stakeholders and citizens, and to take into account ethical, human rights and societal aspects, TRANSCEND will use these to develop or deploy (new) technologies. Critically, these methods facilitate collaboration, e.g., with industry, government, academia, and CSOs / citizens.	TRANSCEND will provide a set of methods to promote collaboration between security professionals, industry, academia, and CSOs / citizens. Critically, you can require them to follow these methods when you fund their projects.	TRANSCEND will provide a set of methods to contribute to the development and/or deployment of (new) technologies. Critically, these methods facilitate collaboration, e.g., with security practitioners, industry, government, and CSOs / citizens.	TRANSCEND will provide a set of methods in order to contribute to the development and/or deployment of (new) technologies. Critically, these methods can empower you to collaborate with, e.g., security practitioners, industry, academia, and government.	TRANSCEND will provide a set of methods in order to develop or deploy (new) technologies in your project, and to organize collaboration between security professionals, industry, government, academia, and CSOs / citizens (Quadruple Helix).

Table 13: Key messages - WP1

WP2 - STAKEHOLDER MAPPING, NETWORKING, MUTUAL LEARNING AND TRAINING TO ENHANCE CITIZEN AND SOCIETAL ENGAGEMENT	Security Practitioners	Policy Makers	Research Organisations	Citizens/The public, NGOs, CSOs and Media	Other Relevant EC funded projects
OBJECTIVES	**KEY MESSAGES**				
Map the European landscape of CSOs engaged in security research both nationally and at the	This objective will be pursued through the publication of	This objective will be pursued through the publication of a public report –	This objective will be pursued through the publication of a public report –	This objective will be pursued through the publication of a public report –	N/A

EU level and identify and develop strategies to further engage the civil society with security research in Europe	a public report – selected security practitioners will be contacted to let them know about the publication.	selected policy makers might will be contacted to let them know about the publication.	selected research organizations will be contacted to let them know about the publication.	selected NGOs will be contacted to let them know about the publication.	
Create and sustain a network of CSOs, and promote continuous dialogue between the network and end-users of security research	Some practitioners will be invited to join these networks	Some policy makers might be invited to join these networks	N/A	Some NGO representatives will be invited to join these networks	N/A
Develop training modules for CSOs and end-users of security research products to promote societally responsible innovation in security research	Will be contacted to join these training sessions	will be contacted to join these training sessions	will be contacted to join these training sessions	will be contacted to join these training sessions	N/A
Continually engage with other tasks in the project to promote continuous impact throughout the different phases of the project	N/A	N/A	N/A	N/A	N/A

Table 14: Key messages - WP2

WP3 – PILOTING STAKEHOLDER ENGAGEMENT IN SECURITY RESEARCH	Security Practitioners	Policy Makers	Research Organisations	Citizens/The public, NGOs, CSOs and Media	Other Relevant EC funded projects
OBJECTIVES	**KEY MESSAGES**				
Implement, test and validate a methodology for stakeholder-engaged responsible R&D in four security research domains.	Citizen engagement is not rocket science: TRANSCEND has developed a toolbox with methods that can also be implemented in practical work and produce useful results. TRANSCEND shows ways for citizens and	Citizen engagement is meaningful and feasible: TRANSCEND has shown that security research can capture citizens' needs and reduce concerns through the use of appropriate methods.	A) Citizen engagement is not rocket science: TRANSCEND has developed a toolbox with methods that can also be implemented in practical work and produce useful results. TRANSCEND shows ways for citizens and companies to collaborate in a special	R&D takes citizens' opinions seriously and involves citizens in the development process in security research OR Research takes the opinions of citizens seriously and is able to involve citizens in the development of security solutions.	Citizen engagement is not rocket science: TRANSCEND has developed a toolbox with methods that can also be implemented in practical work and produce useful results. TRANSCEND shows ways for citizens and companies to

	companies to collaborate in a special knowledge and innovation ecosystem.		knowledge and innovation ecosystem. B) Citizen engagement is meaningful and feasible: TRANSCEND has shown that security research can capture citizens' needs and reduce concerns through the use of appropriate methods.		collaborate in a special knowledge and innovation ecosystem.
Carry out pilots in the security domains of cybersecurity (CS), disaster resilient societies (DRS), fighting crime and terrorism (FCT) and border management (BM)	Participate and share your expertise!	N/A	Volunteer as pilot and share your expertise!	Participate and share your knowledge!	Volunteer as pilot!
Provide insights based on the pilots into societal impacts, problems and possible solutions in the different areas of security research	Apart from the proof of the concepts for citizen engagement, TRANSCEND will also identify important issues in all 4 application areas under consideration that are important to citizens and should be addressed or improved in further research. This will allow assessing the impact and will promote an active, deliberate dialogue between citizens, security practitioners stakeholders and public decision-makers.				

Table 15: Key messages - WP3

WP4 – CREATE IMPACT: DISSEMINATE, COMMUNICATE AND EXPLOIT RESULTS	Security Practitioners	Policy Makers	Research Organisations	Citizens/The public, NGOs, CSOs and Media	Other Relevant EC funded projects
OBJECTIVES	**KEY MESSAGES**				
Identify and develop suitable strategies to disseminate, communicate, engage with and raise awareness	Sharing projects findings and capitalise them will be an essential aspect the project activities. This	To be aware of the main results of TRANSCEND and to provide a set of recommendations based on the	Sharing projects findings and capitalise them will be an essential aspect the project activities. This	Use suggestions and recommendations which will be implemented during the project linked to	Several cooperation modalities such as organisation and participation

in the project's distinct target audiences	target audience will be aware of all the progresses and results, and it will have access to them.	experience of the project and make the best possible use of the outcomes of the Policy-research dialogues and initiatives.	target audience will be aware of all the progresses and results, and it will have access to them.	continuous engagement, cooperation and joint activities.	to joint workshops, conferences and events will increase the level of knowledge exchange between TRANSCEND and other relevant EC projects at European level
Recognise and use exploitable results and avenues for exploitation activities and concretise the value and impact of research and collaboration for sustainability	TRANSCEND Toolbox and Framework, Recommendations for ethical, human rights and social impact assessments, TRANSCEND Network and Training and mutual learning modules will be exploited and presented.	Recommendations for ethical, human rights and social impact assessments will be exploited and a set of policy briefs and recommendation will be presented.	TRANSCEND Toolbox and Framework, Recommendations for ethical, human rights and social impact assessments, TRANSCEND Network and Training and mutual learning modules will be exploited and presented.	Method to evaluate and promote citizen and societal engagement and Training and mutual learning modules will be shared and exploited in order to maximise the possibility to use them in further research.	Potential cooperation activities will be conducted in order to provide and guarantee a sustainable strategy especially beyond the project duration.
Synthesise results and create a powerful and effective framework for designing an inclusive and context-sensitive stakeholder and citizen and societal engagement, which includes a Toolbox to give it practical shape	TRANSCEND will have an impact especially after the first activities and results. A summary of results and activities will be a crucial element in the project's context, especially in regard to the engagement at general, and local level, taking into account the four pilots of the project.	Synthesise the project's results will have a crucial impact on Policy and decision makers at local, national and European level. New recommendations and policy papers will be developed and implemented in order to provide new knowledges and decisions based on the results of TRANSCEND will be taken in consideration.	A shared learning will be an important aspect in the TRANSCEND context, and the results will be re-launched at different levels in order to guarantee and integrate new expertise and knowledges. The research organisation already included in TRANSCEND will act a fundamental role in order to engage, disseminate and shape the new knowledges and findings.	TRANSCEND will have an impact especially after the first activities and results. A summary of results and activities will be a crucial element in the project's context, especially in regard to the engagement at general, and local level, taking into account the four pilots of the project.	Several cooperation modalities such as organisation and participation to joint workshops, conferences and events will increase the level of knowledge exchange between TRANSCEND and other relevant EC projects at European level

Table 16: Key messages - WP4

5 Dissemination and Communication Plan for engagement

5.1 Timeline

For a better impact, the Dissemination and Communication Plan will follow several phases in terms of implementation:

Awareness phase, Initial Phase from M1 to M9: Between M1 and M9, awareness for TRANSCEND will be raised, the project needing to be visible and recognisable, sharing main aims and values. Social media channels, visual identity, templates, 1st factsheet and website will be all set up by M6. From M6 to M9, the consortium will get familiar with the tools in place.
Channels & Tools: Website, Twitter and LinkedIn[4] channels, Factsheets

1st Intermediate Phase / M10-18: Between M10 and M18, the 1st Intermediate Phase will take care of the dissemination aspects by increasing interest to targeted communities, presenting the aim and early results of TRANSCEND in targeted conferences and events (Please see Annex 4). Communication actions will continue leveraging the potentials of Twitter and LinkedIn, website and future newsletters. Creating strong links with other projects is also a goal to pursue between M10 and M18.
The first Annual conference will be organised at M12.
Channels & Tools: Website, newsletters, Twitter and LinkedIn channels, annual conference, Networks, participation in conferences, publications, Media Toolkit

2nd Intermediate Phase / M19 – M27: Between M19 and M27, the consortium will focus on deepening its engagement towards the targeted audiences. Dissemination of evolving results through events will keep creating additional interest in TRANSCEND.
The second annual conference will take place at M24.
Channels & Tools: Website, newsletters, Twitter and LinkedIn channels, annual conference, Networks, participation in conferences, publications

Final Phase / M28-M36: This phase will focus on maximising target market and industry awareness about TRANSCEND's exploitable results. All the results will be disseminated through the aforementioned channels. Communication and dissemination efforts will support the project sustainability and its effective exploitation and market replication.
The final annual conference will be organised at M35.
Channels & Tools: Website, newsletter, Twitter and LinkedIn channels, annual conference, Networks, participation in conferences, publications

[4] The possibility of having a Mastodon account dedicated to TRANSCEND was raised but the consortium decided to focus on Twitter and LinkedIn.

5.2 Dissemination plan: main means

The following section provides an overview of the online and offline dissemination means which will be available to "make [TRANSCEND's] results public"[5].

5.2.1 Online dissemination means

TRANSCEND Website

The project website (http://transcend-project.eu) is the main online tool for public dissemination/communication and serves as the main point of contact for the project. It will be set up in M6 and is managed by Trilateral. It will include information about the project's mission, objectives, workflow, activities, and the consortium. As they become available, the website will be populated with project outputs, news items/blog posts and promotional materials. TRI will ensure it is maintained and updated regularly throughout the project's lifecycle. The website will also prompt visitors to sign up to our newsletter and follow us on social media, thereby aiding us in our goal of obtaining new followers and/or growing our network.
Partners will be invited to contribute by writing blog posts that will be featured in the news section of the website and to actively promote them to the various stakeholder communities. Trilateral and EOS will create guidelines for partners on how to write accessible and easily understandable posts that are suitable for public dissemination.

Online Media Strategy

The main aim of the dissemination strategy is to build and increase awareness as well as improving the general public's understanding of the project and its activities across the security ecosystem. Sharing relevant information related to the TRANSCEND activities will raise interest among the security community in particular and the civil society in general.

5.2.2 Offline dissemination means

Deliverables

TRANSCEND must deliver 18 deliverables, 4 of them are classified as Sensitive and 14 are public. The public documents will be published on the TRANSCEND website once accepted by the EC as well as on the CORDIS website and ZENODO. The detailed description of the results they contain makes their availability to a wide audience crucial.

Project Publications

[5] https://ec.europa.eu/research/participants/docs/h2020-funding-guide/imgs/quick-guide_diss-expl_en.pdf

Open access will be provided to project publications featured in peer-reviewed journals through the 'gold' or green route. The decision will be based on the publisher selected, the scope of the article (results it shares) and the partners who have contributed to the publication. In terms of the green route, the consortium members have agreed that the material will be deposited immediately in an open access repository upon publication, without an embargo period.
Immediate open access of a machine-readable electronic copy through a trusted repository for scientific publications (publisher/Zenodo) at the latest at the time of publication will be ensured for project peer reviewed scientific publications (journal articles/monographs) and TRANSCEND authors will ensure they retain sufficient IPR to fulfil this requirement.

Trainings
Open and free availability of training tools for CSOs and end-users of security research products to promote societally responsible innovation in security research will be made free for download via a sustainable channel to support their use and sustainability.

External Channels
TRANSCEND Results and activities will be shared on several external websites. The consortium already shortlisted the following channels:

- The consortium partners websites and social media channels through the PoC assigned by each partner (see Annex 1)
- DGs and agencies websites and social media channels

5.2.3 Dissemination through events

Pilot Workshops
Efus Cities will engage with the results of the pilots after they are completed. This dissemination event will be done via virtual workshops.

Support Workshops
These workshops at the national levels will be targeted at policymakers, local authorities from other cities and/or regions, advocacy campaigns to increase the involvement of civil society and citizens in security tech research. 4 events will be organised to ensure this dissemination.

Third-party events and conferences

The Annex 6.4 lists potential events which could be interesting to attend. For some of these events, TRANSCEND will be invited to present its main outputs, for others the idea would be to meet relevant stakeholders or consortium members from other projects in order to exchange lessons learned and best practices.

5.2.4 Synergies with other relevant projects

The creation of synergies with other relevant EU or national projects is key to increase the visibility of TRANSCEND and put in place a proper exchange of information, avoiding any work duplication and sharing experience and lessons learned. The links created between TRANSCEND and other projects can be seen as a mutual promotion of news, mutual invitation to participate and present project workshops or organise joint events.

5.3 Communication plan: main means

According to the EC, communicating concerns "promoting [TRANSCEND's] action[s] and results"[6]. The subsections below present concrete measures which will be implemented throughout the project timeline.

5.3.1 Visual Materials

The project's visual identity is the brand of the project and is defined by the logo (Annex 2, provided by TRI at the proposal stage), the colour codes (Annex 2) and the document templates (Annex 3, provided at M1 by EOS).

A promotional package will be designed and will include:
- A factsheet document provided by EOS and TRI, ready at M6
- TRANSCEND roll-ups (at least 2) to be showcased during projects events, ready at M6
- Promotional leaflets with the description of the main objectives. Both hard and soft copies will be made available and be shared online and during events, from M18. The brochures will also be translated by the partners in their own languages.
- One video will be designed at the end of the project to summarise the main outputs of TRANSCEND

[6] quick-guide_diss-expl_en.pdf (europa.eu) consulted on the 8th of February 2023

Figure 1: 1st TRANSCEND Factsheet

5.3.2 TRANSCEND Website

As explained in the previous section, the website is our main online tool for public dissemination/communication. As such, we will ensure it is accessible by a wide audience and through several devices: computers, tablets, smartphones. It will share information about TRANSCEND, its partners, its main outputs, objectives and related activities.

5.3.3 TRANSCEND Social media strategy

Developing a working strategy for social media is crucial as most of the actors in the security field are using such media to communicate and share insights, as the necessity to get and receive the information as fast and as simply as possible is increasing. The posts on both Social media (LinkedIn and Twitter, see below) will synchronised, but their contents will differ due to the limits imposed by the platforms.

Social media also enhances a more concrete level of exchange than a simple website, giving an impression of proximity. Social media platforms allow readers to "stay in touch" and their use by different stakeholder groups will raise TRANSCEND's presence online. TRANSCEND Social media channels are operational since November 2022 (M2). A LinkedIn profile, called TRANSCEND Horizon Europe has been set up to share and promote activities with the different stakeholders connected: practitioners, industry representatives or research and scientific networks. It is managed by EOS with input sent from all the partners whenever they consider it relevant. The content to be presented on Social Media channels will consist in TRANSCEND outputs, news from the academic community on the involvement of CSO for security technologies development and deployment as well as activities carried by partners relevant to the actions. Moreover

starting from M8, partners will work on bi-monthly blogposts to be published on the website and social media.
Finally, consortium partners will repost what has been shared on the project website and on their social media channels (listed in Annex 1).

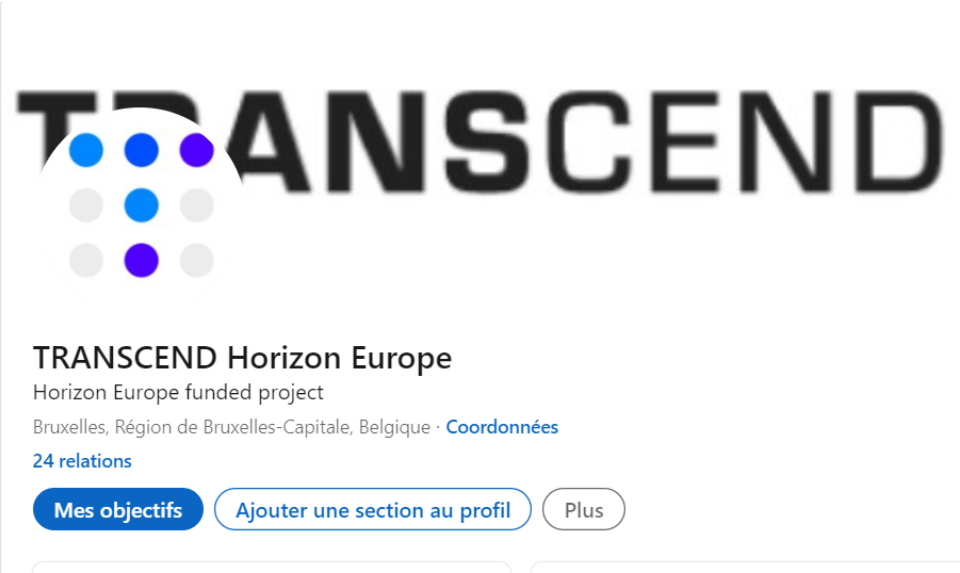


Figure 2: Screenshot TRANSCEND LinkedIn account

Through a Twitter account, @TranscendHEu, insights into the project's immediate activity are shared with the "Followers". Twitter is well known to engage with a wide audience on an hour-to-hour basis and raise an instant interest in the stories shared. The content of the Twitter account needs to be updated regularly and relevant hashtags are used to enhance the visibility of the tweets.

Figure 3: Screenshot TRANSCEND Twitter Account

Finally, contents will be shared on Social Media on a monthly basis, and up to two times a month depending on project outputs and relevant activities to be communicated.

5.3.4 Newsletter

The project's newsletter will be shared every 6 months among the consortium and the relevant targeted network, presenting the project's main achievements and upcoming activities. The contact list will be developed through the activities from WP2, especially T2.1 (Map relevant stakeholders, networks & projects) and T2.2 (Initiate, coordinate the TRANSCEND Network, Stakeholder Board and clustering activities) which aims at developing the TRANSCEND Network, and T4.1 (Dissemination and communication plan and activities). The common development of the contact list, using the outputs of several task across two Work Packages, will ensure its robustness and consistency. Once the stakeholders and TRANSCEND Network members contact points are identified, the newsletter will be shared using tools such Sendinblue or Mailchimp. The first edition of the newsletter will be released at M7, instead of M6 as initially planned, and will include an introduction to the project and the very first outcomes of TRANSCEND. The decision to delay the first issue (by 1 month) was motivated by the publication of the result of T1.1 (State of the art in methods for citizen and societal engagement) due to M7. The document will be shared among consortium members who will also share it with their network. It will also be posted on the TRANSCEND website.

5.4 TRANSCEND Visual Identity and Social Media Communication Guidelines

The Visual Identity and Social Media Communication Guidelines have been drafted by EOS and shared with the consortium at M4 (Annex 5).
The target audience of the document is TRANSCEND consortium partners. It aims at including all logo, text and style guidelines needed to create TRANSCEND documents for print or web as well as providing them with a basic knowledge of what social media is, their difference and use.

5.5 TRANSCEND Crisis Communication Plan

The TRANSCEND Crisis Communication Plan has been drafted by EOS, with the support of TRI, and shared with the consortium at M6 (Annex 6).
The document is designed to allow TRANSCEND partners to quickly and effectively respond in the event of an emerging threat to the project's reputation. Journalists or representatives from civil society might voice some concerns regarding the project's objectives, results or methods. In this case, the project must be able to react fast enough through a coordinated approach. This document provides clear and brief guidelines for TRANSCEND partners to guide them in case they are contacted by a third party who might want to disseminate false, inaccurate or misinterpreted information about the project in the news media.

6 Monitoring and Evaluation

In order to maximise impact, dissemination and communications activities need to be properly evaluated.

The Plan for dissemination and communication has to be seen as an evolving document which will be updated at M20.

EOS will be in charge of monitoring dissemination and communication activities as WP4 leader, through a Dissemination log (Annex 7) and a monitoring spreadsheet (Annex 8) which will facilitate collating all relevant data, both in terms of activities and the audience reached through the project's outputs. The monitoring sheet and Dissemination log are saved in the TRANSCEND SharePoint and has to be updated with the relevant information recording the type of dissemination activities and their achieved impact, in terms of estimated reached audience.

EOS needs to regularly check the status of the monitoring record with the partners involved in dissemination and communication activities and starting from M6 send monthly reminders to partners to update the spreadsheet. The regular use of the monitoring tool will provide updates on achieving impact and reaching our targets (KPIs) which are listed below:

Channels/Tools	Indicators	Type of data used	KPIs
Website	Number of visitors	Google analytics	100 visitors per month
Social Media	Members of LinkedIn group	LinkedIn Group Statistics	Minimum of 200 at M19
	n. of Twitter followers	Twitter analytics	Minim of 200 at M19
Newsletter	n. of Newsletter published	N/A	6
Video	n. of videos released	N/A	1
Workshops	n. of participants	List of participants	50 for physical events
Final event	n. of participants	List of participants	80
Scientific publications	n. of scientific publications submitted	Proceedings	Up to 4 at M19
Liaison activities and synergies	n. of relevant projects/initiatives identified and invited at project events	List of participants	5 per event
Third-party event attendance	n. of relevant events attended	Proceedings	6 at M19

Table 17 – KPIS

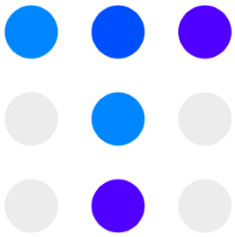
7 Annexes

7.1 Annex 1 - TRANSCEND partners' social media accounts

Partners	Twitter	LinkedIn
TRI	@TRIResearch_	Trilateral Research
TNO	@TNO_Research	TNO
Fraunhofer	@FraunhoferISI	Fraunhofer ISI
EOS	@EOS_EU	EOS
EFUS	@Efusnews	Efus
PRIO	@PRIOresearch	N/A
AutRC	@roteskreuzat	Österreichisches Rotes Kreuz
Code for All	@CodeforAll	https://www.linkedin.com/company/code-for-all/

Table 18: TRANSCEND partners' social media accounts

7.2 Annex 2 - TRANSCEND Logo and colour Palette



TRANSCEND

Figure 4: TRANSCEND High Resolution Logo

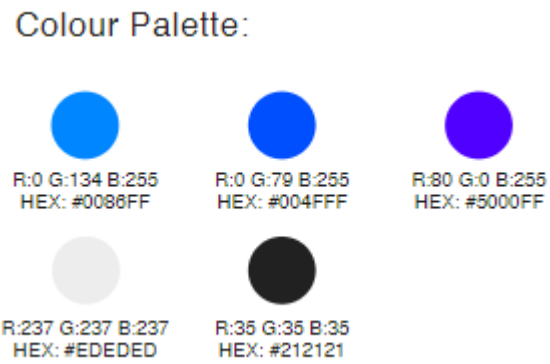
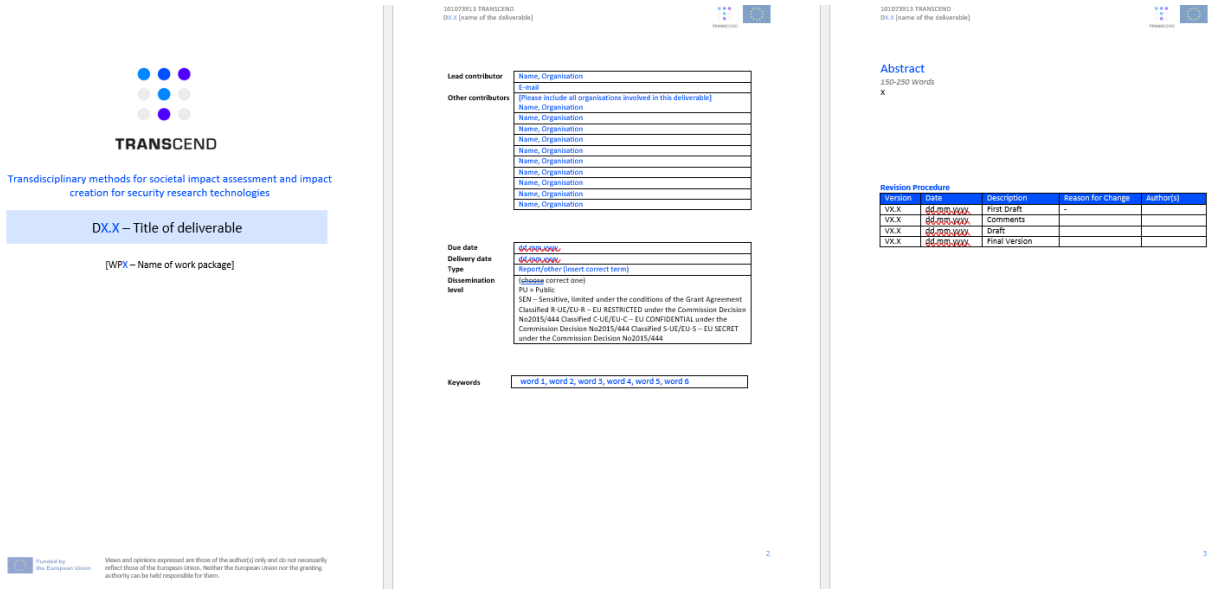
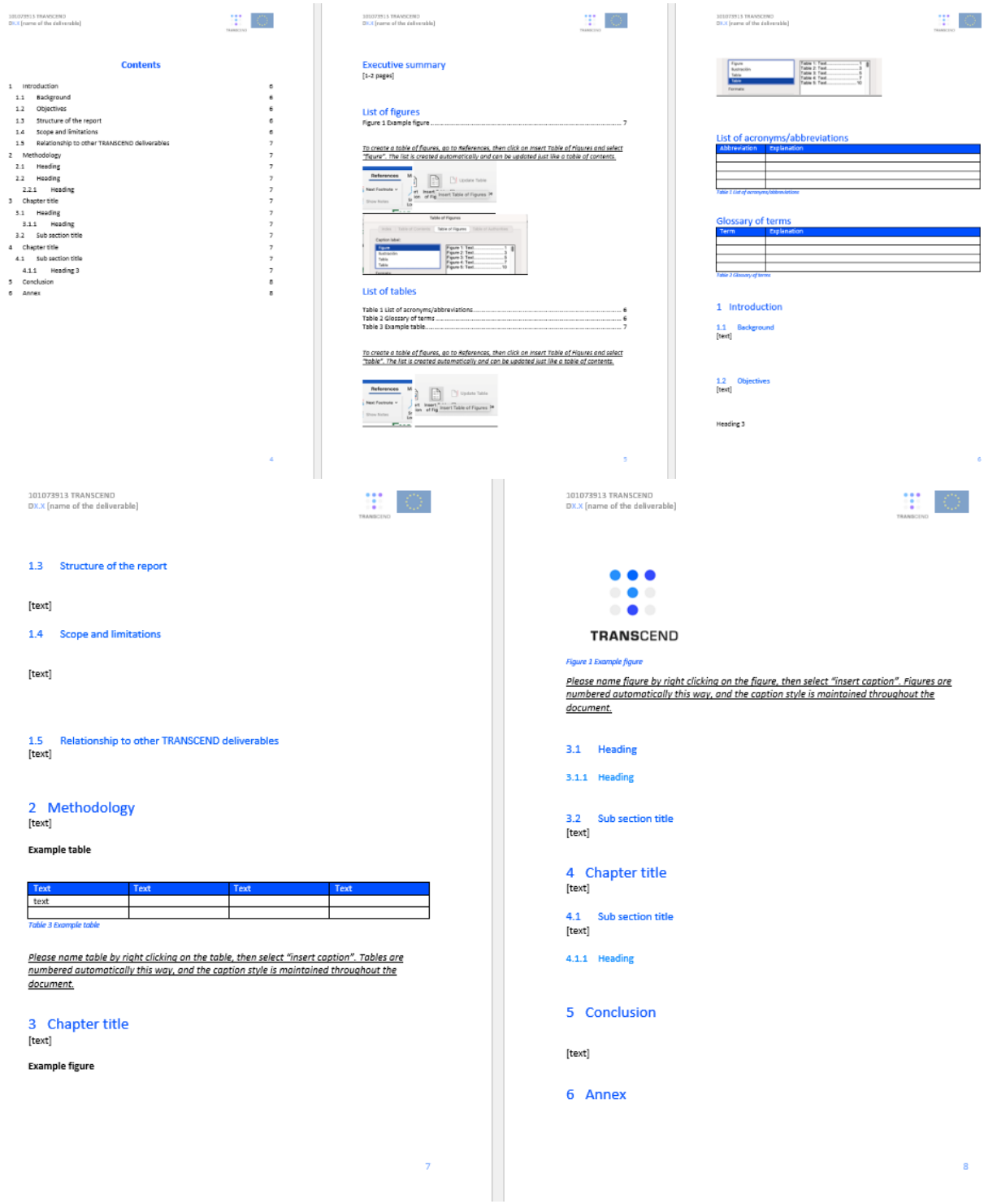


Figure 5: TRANSCEND Colour Palette

7.3 Annex 3 – TRANSCEND Templates





Contents

1 Introduction 6
1.1 Background 6
1.2 Objectives 6
1.3 Structure of the report 6
1.4 Scope and limitations 6
1.5 Relationship to other TRANSCEND deliverables 7
2 Methodology 7
2.1 Heading 7
2.2 Heading 7
2.2.1 Heading 7
3 Chapter title 7
3.1 Heading 7
3.1.1 Heading 7
3.2 Sub section title 7
4 Chapter title 7
4.1 Sub section title 7
4.1.1 Heading 3 7
5 Conclusion 8
6 Annex 8

Executive summary
[1-2 pages]

List of figures
Figure 1 Example figure 7

To create a table of figures, go to References, then click on Insert Table of Figures and select "Figure". The list is created automatically and can be updated just like a table of contents.

List of tables
Table 1 List of acronyms/abbreviations 6
Table 2 Glossary of terms 6
Table 3 Example table 7

To create a table of figures, go to References, then click on Insert Table of Figures and select "Table". The list is created automatically and can be updated just like a table of contents.

List of acronyms/abbreviations

Abbreviation	Explanation

Table 1 List of acronyms/abbreviations

Glossary of terms

Term	Explanation

Table 2 Glossary of terms

1 Introduction
1.1 Background
[text]
1.2 Objectives
[text]
Heading 3

101073913 TRANSCEND
DX.X [name of the deliverable]

1.3 Structure of the report
[text]
1.4 Scope and limitations
[text]
1.5 Relationship to other TRANSCEND deliverables
[text]

2 Methodology
[text]
Example table

Text	Text	Text	Text
text			

Table 3 Example table

Please name table by right clicking on the table, then select "insert caption". Tables are numbered automatically this way, and the caption style is maintained throughout the document.

3 Chapter title
[text]
Example figure

TRANSCEND

Figure 1 Example figure

Please name figure by right clicking on the figure, then select "insert caption". Figures are numbered automatically this way, and the caption style is maintained throughout the document.

3.1 Heading
3.1.1 Heading
3.2 Sub section title
[text]
4 Chapter title
[text]
4.1 Sub section title
[text]
4.1.1 Heading
5 Conclusion
[text]
6 Annex

Figure 6: Screenshot TRANSCEND Deliverable Template

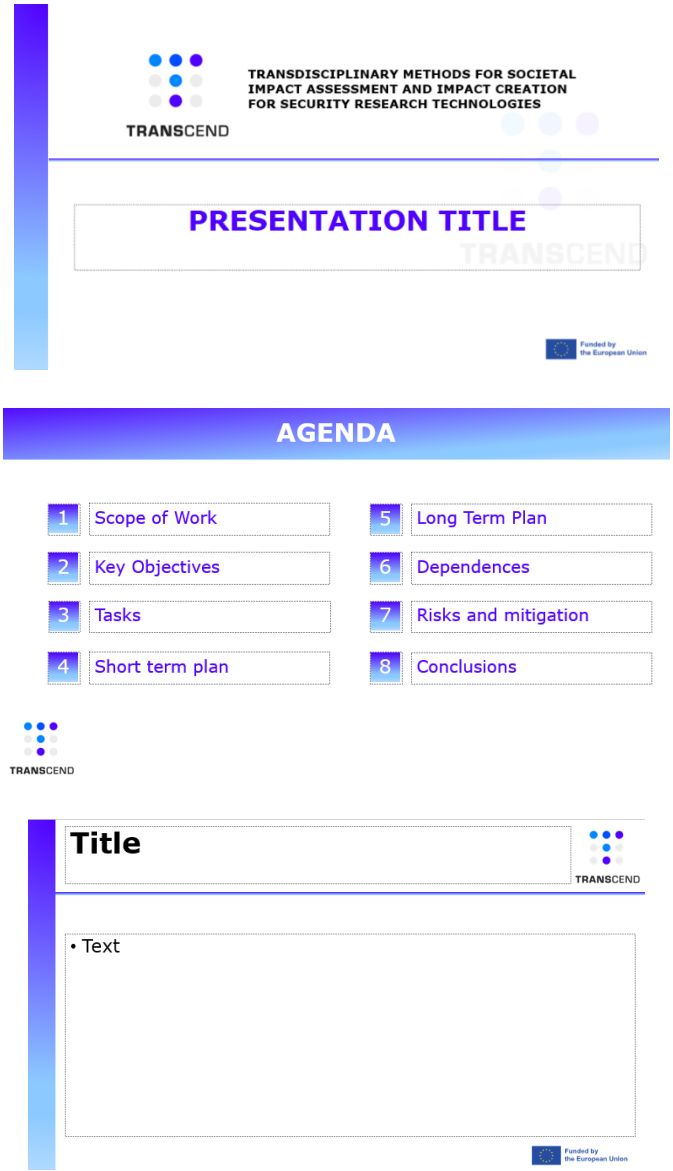


Figure 7: Screenshot TRANSCEND PPT Presentation Template

7.4 Annex 4 – List of relevant events to attend

Events Attended/Forthcoming

Name of the event (full name)	Date	Place	Partner(s) Attending (top-down)			Activity (top-down, if other, use description)	Output description - report	Follow-up Actions (if needed)
Mozilla Festival	March 20-24	Virtual	CfALL	-	-	Festival	-	-

World Ethical Data Forum		TBC	CfALL	-	-	Conference	-	-
RightsCon	June 5-8	Costa Rica	CfALL	-	-	-	-	-
Internet Freedom Festival		TBC	CfALL	-	-	Festival	-	-
Personal Democracy Forum		TBC	CfALL	-	-	Conference	-	-
OSCE Security Days		TBC	CfALL	-	-	Conference	-	-
Freedom not Fear	September 1-4	Brussels - BE	CfALL	-	-	-	-	-
Privacy Camp	January 2024	Brussels - BE	CfALL	-	-	-	-	-
CERIS DRS European Forum on Risk Governance & Societal Resilience	16-17th May 2023	Toulouse - FR	EOS	-	-	Conference	-	-
SMI2G	10-11th May 2023	Paris – FR	EOS	TNO	-	Workshops	-	-
PRECINCT Conference	16-17th May 2023	Brussels - BE	EOS	-	-	Conference	-	-
CERIS Project to Policy Seminar	14-15th June 2023	Brussels – BE	TRI	EOS	-	Seminar	-	-
CERIS SSRI "Networks of Practitioners" Workshop: Exploitation of outcomes, capability requirements, and future perspectives	27th April 2023	Brussels – BE	EOS	-	-	Workshop	-	-
CERIS Innovation Procurement	5th July 2023	Brussels - BE	EOS	-	-	Conference	-	-
Security Research Event 2023	24 – 25 October 2023	Brussels – BE	TRI	-	-	Annual Meeting/ Exhibition	-	-

Table 19: List of relevant event to attend (tentative)

7.5 Annex 5 – Visual Identity and Social Media Guidelines

TRANSCEND

Transdisciplinary methods for societal impact assessment and impact creation for security research technologies

Visual Identity and Social Media Guidelines

[WP4 – Create impact: Disseminate, communicate and exploit results]

101073913 TRANSCEND
Visual Identity and Social Media Guidelines

Lead contributor	European Organisation for Security – Elodie Reuge, Giacomo Bianchi and Guillaume Brumter
	Elodie.reuge@eos-eu.com, Giacomo.bianchi@eos-eu.com, Guillaume.brumter@eos-eu.com
Other contributors	TRILATERAL

Due date	N/A
Delivery date	N/A
Type	Report
Dissemination level	SEN

Keywords	Communication, dissemination, social media

Contents

1 Visual Identity Guidelines 5
1.1 How to use this Visual Identity style guide 5
1.2 Contact 5
2 Core Visual Identity Elements 5
2.1 European flag and funding statement 5
2.2 Disclaimer 6
2.3 The project logo 6
2.4 The colour code 7
2.5 The font 7
3 Templates 7
3.1 PowerPoint Templates 7
3.2 Word Template 8
4 Social Media guidelines 9
4.1 Why use social media? 9
4.1.1 Communicating vs disseminating 9
4.2 Social Medi Channels 10
4.3 The 4 Cs of Social Media 11

101073913 TRANSCEND
Visual Identity and Social Media Guidelines

Executive summary

This guidelines have by WP4 leader, the European Organisation for Security. Its target audience is TRANSCEND consortium partners and aims at including all logo, text and style guidelines needed to create TRANSCEND documents for print or web as well as providing them with a basic knowledge of what social media is, their difference and use.

List of figures

Figure 1 Example figure 7

List of tables

Table 1 List of acronyms/abbreviations 4
Table 2 Glossary of terms 4
Table 3 Example table 7

List of acronyms/abbreviations

Abbreviation	Explanation
DC	Dissemination and Communication
GA	Grant Agreement

Table 1 List of acronyms/abbreviations

Glossary of terms

Term	Explanation

Table 2 Glossary of terms

[text]

1 Visual Identity Guidelines

1.1 How to use this Visual Identity style guide

The TRANSCEND visual identity guidelines aim to create a unique and recognisable image of the project. It supports the coherent and consistent use of tis visual elements in all TRANSCEND Dissemination and Communication (DC) materials. This includes publications, presentations and other marketing materials (offline and online). Guidelines on the correct use of the logo, the fonts, colours and templates are included.
Consortium partners should use and follow these guidelines in all DC activities related to TRANSCEND. Documents related to the project should include the Grant Agreement (GA) number (101073913), EU logo, funding acknowledgement and project logo.

1.2 Contact

If you are unsure about how to apply the guidelines in a particular case, please contact Guillaume Brumter, Giacomo Bianchi or Elodie Reuge at EOS:
Guillaume.brumter@eos-eu.com, Giacomo.bianchi@eos-eu.com and Elodie.reuge@eos-eu.com

2 Core Visual Identity Elements

2.1 European flag and funding statement

All TRANSCEND partners, as recipients of EU funds, are under a legal obligation to acknowledge the support from the European Union on all communication materials.
According to Article 17.2 of the GA, the European flag an funding statement must be displayed prominently on all TRANSCEND related printed or digital materials, websites, social media channels etc:

Figure 1 EU emblem and funding statement

If needed, the EU flag and funding statement may also be displayed in local languages. EU emblem translations can be found here.
The minimum height of the emblem must be 1 cm with exceptions for specific items (such as pens etc).

5

The statement 'funded by the European Union' must always be included. In addition, in written communication TRANSCEND partners should acknowledge the GA number, as follows:

Funded by the European Union.
UK based consortium partner Trilateral Research Limited, UK is funded by UK Research and Innovation (UKRI) under the UK government's Horizon Europe funding guarantee [grant number 101073913]. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency or UKRI. Neither the European Union nor the granting authority can be held responsible for them.

2.2 Disclaimer

All TRANSCEND related communication or dissemination activities must indicate at least the following disclaimer (translated in local languages where appropriate):

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

Or

"This document has been produced in the context of the TRANSCEND Project. This project is part of the European Union's Horizon Europe research and innovation programme and is as such funded by the European Commission. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. All information in this document is provided 'as is' and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. For the avoidance of all doubts, the European Commission has no liability with respect to this document, which is merely representing the authors' view."

2.3 The project logo

The TRANSCEND logo may be used in two forms, as a complete logo or as a compact logo in case of limited space:

TRANSCEND

Figure 2 TRANSCEND complete logo

Figure 3 TRANSCEND compact logo

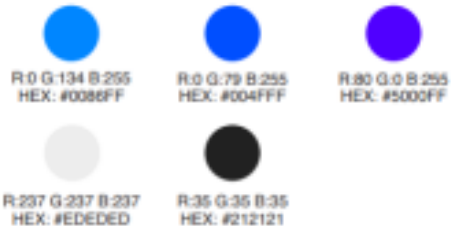
Do's and Don'ts

The correct proportions of the logo have to always have to be respected in case of change in the size of the logo, **do not:**

- Distort the logo
- Reduce the size of the complete logo where the name of the project is not visible
- Add design effects
- Place any elements on the logo / remove elements of the logo

2.4 The colour code

The following distinctive colours of the project should be used according to RGB and HEX codes below:



2.5 The font

The Verdana font has been chosen so partners would not need to install any special fonts on their computers. Normal text size should be at least 12 pt.

3 Templates

3.1 PowerPoint Templates

The PowerPoint Template has been created and shared with the partners in November 2022.
All presentations both for internal and external audiences must use the template. Depending on the content of the presentation, there are various slide types available in the template.

Figure 4 First slide of the PPT Template

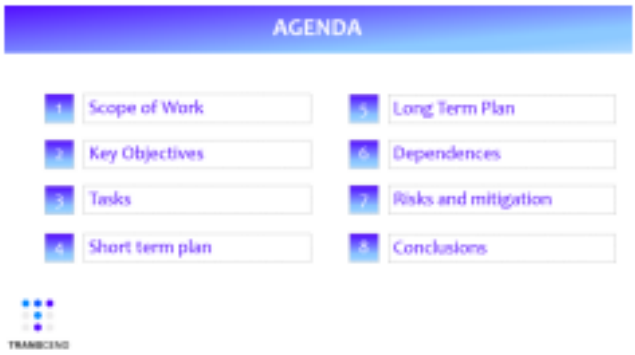


Figure 5 Second slide of the PPT presentation

3.2 Word Template

The deliverable template has also been shared with the partners in November 2022.
For word documents, the font used should Verdana.

TRANSCEND

Transdisciplinary methods for societal impact assessment and impact creation for security research technologies

DX.X – Title of deliverable

[WPX – Name of work package]

Lead contributor	Name, Organisation
	E-mail
Other contributors	[Please include all organisations involved in this deliverable]
	Name, Organisation
	Name, Organisation
	Name, Organisation
	Name, Organisation
	Name, Organisation
	Name, Organisation

Due date	dd.mm.yyyy
Delivery date	dd.mm.yyyy
Type	Report/other (insert correct term)
Dissemination level	PU = Public PP = Restricted to other programme participants (including the Commission Services) RE = Restricted to a group specified by the consortium

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101073913.

Figure 6 First page of the deliverable template

4 Social Media guidelines

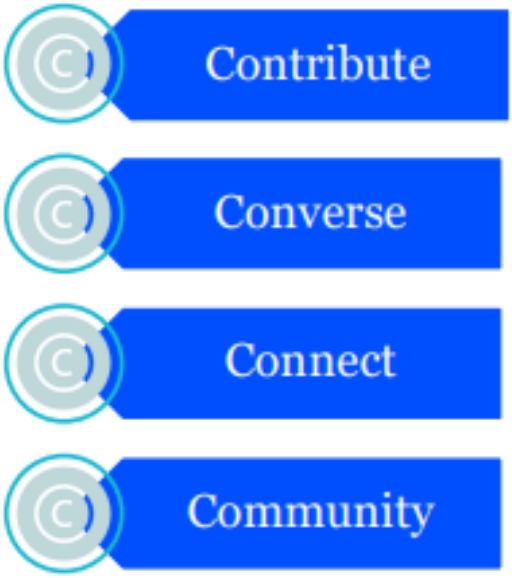
4.1 Why use social media?

Social Media allow the user to reach a wide and targeted audience, to maximise the impact and ensure a successful exploitation of TRANSCEND research results.

4.1.1 Communicating vs disseminating

Social media channels can be used both for communication and dissemination activities.
The differences between both are explained in the table below:

4.3 The 4 Cs of Social Media



1) Contribute: share useful content already produced or not.

2) Converse: listen and respond, contribute to the discussion, this can expend the sphere of influence of the project.

3) Connect: priories and come together with others. Target groups who could spread your message.

4) Community: build relations with people

- **Twitter**
  - ***What can be posted?***

Text up to 280 characters can be shared. This excludes media attachments and quoted tweets (displaying someone else's tweet within your own) but includes links (a URL is always altered to 23 characters).

  - ***How can it be used?***

To share short and catchy messages or comments, make announcements that can instantaneously reach a large audience or retweet relevant content.

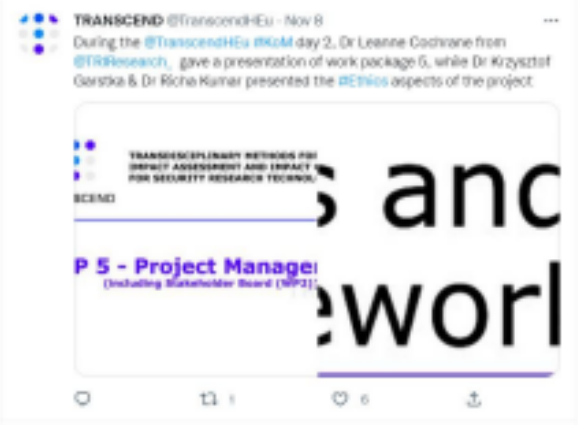


Figure 7 Example of a Tweet

- **LinkedIn**
  - ***What can be posted?***

Text without any character limit, photos, documents, links, videos etc.

  - ***How can it be used?***

A networking site for professionals, it can be used for groups and has established networks on specific topics. TRANSCEND has chosen to create a LinkedIn profile to share content and connect with already established groups.

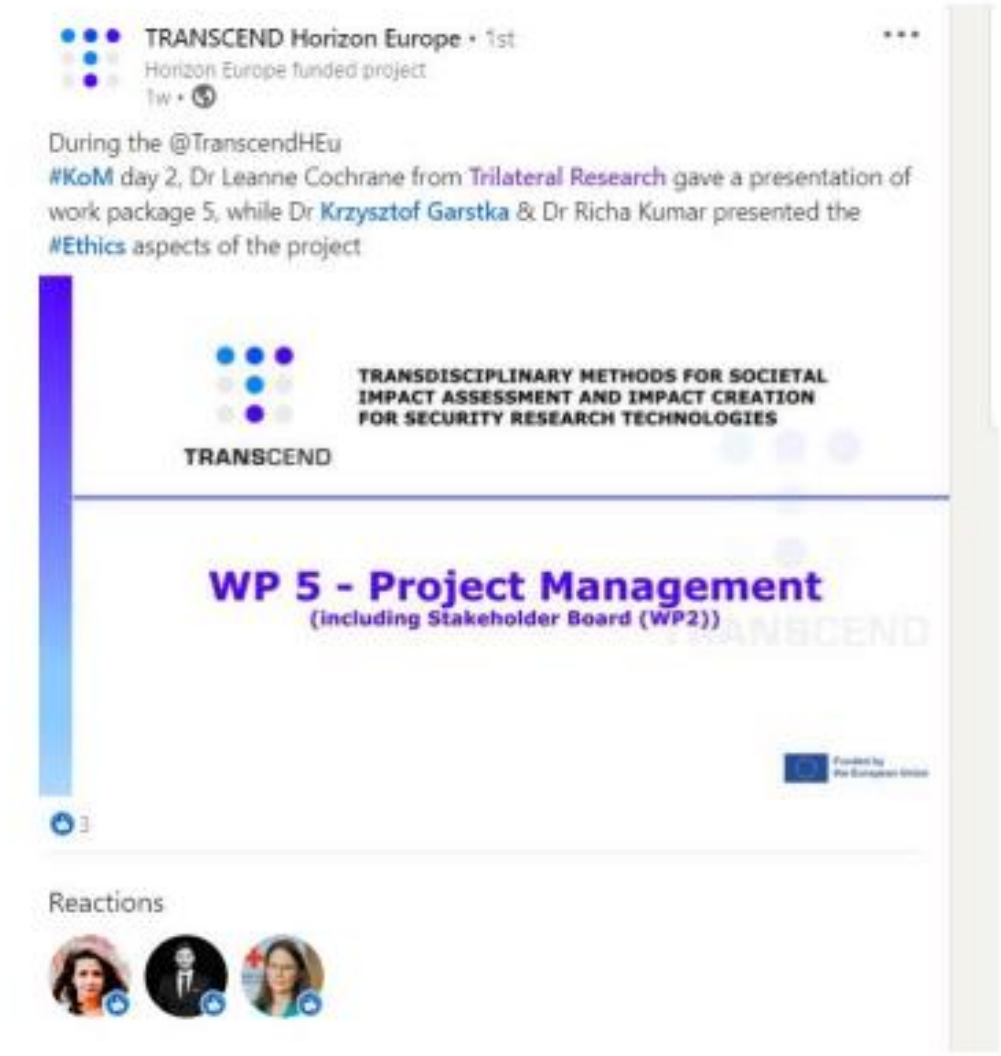


Figure 8 Example of LinkedIn post

- **Who is in charge?**

EOS is the partner leading WP4. EOS already set up the TRANSCEND social media channels and manages the TRANSCEND Twitter and LinkedIn profiles, centralises the data to share and, together with TRI, communicates with the audience.

However, it is important to underline that DC tasks are a shared responsibility and as such regular exchange of information between the consortium and EOS is a necessity.

The DC strategy will be used to collect the DC Points of Contacts of the consortium organisation, as well as their social media channels. The PoCs

will give inputs, validate post if needed, while EOS will be in charge of uploading content.

- **Security aspects**

TRANSCEND, through one of its Partners the European Organisation for Security, EOS, (EU Transparency Register: 32134385519-64) will be using social media like: Twitter, LinkedIn and YouTube. Please find below some clarifications related to the data protection provisions about the application and use of these social media accounts.

  - **Twitter**

The controller, EOS, has integrated components of Twitter. Twitter, as explained above is a multilingual, publicly available microblogging service on which users may publish and spread so-called "tweets", e.g. short messages, which are limited to 280 characters. These short messages are available for everyone, including those who are not logged on to Twitter. The tweets are also displayed to-so called followers of the respective user. Followers are other Twitter users who follow a user's tweets. Furthermore, Twitter allows you to address a wide audience via hashtags (#), links or retweets.

The operating company of Twitter is Twitter, Inc., 1355 Market Street, Suite 900, San Francisco, CA 94103, UNITED STATES.

The controller will make available on the TRANSCEND website a Twitter component (Twitter button). Once a user clicks on the button, the Internet browser on their information technology system is automatically prompted to download a display of the corresponding 'tweeting' component of Twitter.

Further information about the Twitter buttons is available under https://developer.twitter.com/en/docs/twitter-for-websites/tweet-button/overview. The applicable data protection provisions of Twitter may be accessed under https://twitter.com/privacy?lang=en.

  - **LinkedIn**

The controller, EOS, has integrated components of LinkedIn. LinkedIn, as explained above, is a multilingual, publicly available that allows for professional networking, by allowing people to create a profile where to upload a Curriculum Vitae, and set up organisation accounts, participate in conversation, share messages, position papers. This information is available

for everyone, including those who are not logged in to LinkedIn. The posts are also displayed to so-called connections of the respective account.

To set-up a business profile of TRANSCEND, the controller has delegated to two of employees, Angeliki Tsanta and Elodie Reuge, the right to manage the profile.

The operating company of LinkedIn is LinkedIn, 1000 W Maude Ave. Sunnyvale, CA, 94085-2810 UNITED STATES.

The controller will make available on TRANSCEND website a LinkedIn component (LinkedIn button). Once a user clicks on the button, the Internet browser on their information technology system is automatically prompted to download a display of the corresponding LinkedIn profile.

Further information about the applicable data protection provisions of LinkedIn may be accessed under https://www.linkedin.com/legal/privacy-policy.

Figure 8: Visual identity and social media guidelines

7.6 Annex 6 – Crisis Communication Plan

TRANSCEND

Transdisciplinary methods for societal impact assessment and impact creation for security research technologies

Crisis Communication Plan

[WP4 – Create impact: Disseminate, communicate and exploit results]

Funded by the European Union

Funded by the European Union.
UK based consortium partner Trilateral Research Limited, UK is funded by UK Research and Innovation (UKRI) under the UK government's Horizon Europe funding guarantee [grant number 101073913]. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency or UKRI. Neither the European Union nor the granting authority can be held responsible for them.

101073913 TRANSCEND
Crisis Communication Plan

Lead contributor	Elodie Reuge, Guillaume Brumter, Giacomo Bianchi, European Organisation for Security
	Elodie.reuge@eos-eu.com; Guillaume.brumter@eos-eu.com; Giacomo.bianchi@eos-eu.com
Other contributors	N/A
	Name, Organisation
	Name, Organisation
	Name, Organisation
	Name, Organisation

Due date	N/A
Delivery date	N/A
Type	Report
Dissemination level	SEN

Keywords	Crisis, communication, dissemination, actions, contact points

Contents

1 TRANSCEND Points of Contact....3
2 Strategy to adopt in case of crisis....3
3 Scenario 1....4
4 Scenario 2....5

Table of figures

Figure 1 Scenario 1....4
Figure 2 Response to be used by the consortium partners....5
Figure 3 Scenario 2....5

TRANSCEND Crisis Communication Plan

INTERNAL USE ONLY

The document is designed to allow TRANSCEND partners to quickly and effectively respond in the event of an emerging threat to the project's reputation. Journalists or representatives from civil society might voice some concerns regarding the project's objectives, results or methods. In this case, the project must be able to react fast enough through a coordinated approach. This document provides clear and brief guidelines for TRANSCEND partners to guide them in case they are contacted by a third party who might want to disseminate false, inaccurate or misinterpreted information about the project in the news media.

In brief, the Crisis Communication Points of Contact (POC), together with the coordinator, will be responsible for the mitigation of negative narratives and shall be contacted by other partners in case of a crisis communication event.
The coordinator may then also contact the REA Project Officer in order to inform her/him of any issues, mitigate the potential problem and agree on the needed response in the event of a crisis.

1 TRANSCEND Points of Contact

Partner organisation: European Organisation for Security (EOS)
Role: WP4 Leader
Elodie Reuge, Senior Project Manager: elodie.reuge@eos-eu.com
Giacomo Bianchi, Senior Project Manager: Giacomo.bianchi@eos-eu.com
Guillaume Brumter, Policy and Project Officer: Guillaume.brumter@eos-eu.com

2 Strategy to adopt in case of a crisis

The Crisis Communications Plan aims to mitigate any potential bad publicity which might jeopardise TRANSCEND's objectives, methods and results. As the project's key objectives are to propose, test and evaluate methodologies that can enable citizens and CSOs to participate in the research, development and deployment of technologies and innovations, it is essential to avoid negative publicity as much as possible. At the same time, in the current geopolitical context it is possible that the project and the consortium might be targeted by disinformation campaigns or cyber-attacks. In this respect, it is crucial that all press/third party exchanges are

centralised and all consortium partners are aware in advance of how to proceed.
The scenarios below present how partners are expected to react to enquiries by third parties following a centralised approach to ensure a well-coordinated response. At the same time, this strategy will ensure that criticism from the media or civil society will never be met with silence.

A second key element of crisis communication is informing the consortium and any third parties involved (event participants, network members, etc.) of the situation, the related facts and the response chosen by the POC and the coordinator. This will ensure that they are prepared to react if contacted by inquiring parties. If needed, a template reply specific to the crisis at hand may also be drafted and used by consortium partners.

3 Scenario 1

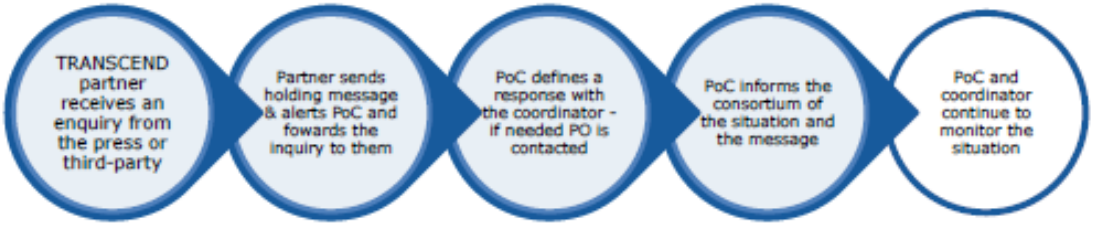


Figure 1 Scenario 1

Partners can use the below message to be sent to third parties as a holding note while the POC prepares a response.

"Dear Sir/Madam,

Thank you very much for your email and your interest in the TRANSCEND activities.

Your request has been forwarded to the appropriate person in the TRANSCEND project consortium, who will get back to you in due course.

Kind regards,

X."

Figure 2 Response to be used by the consortium partners

4 Scenario 2

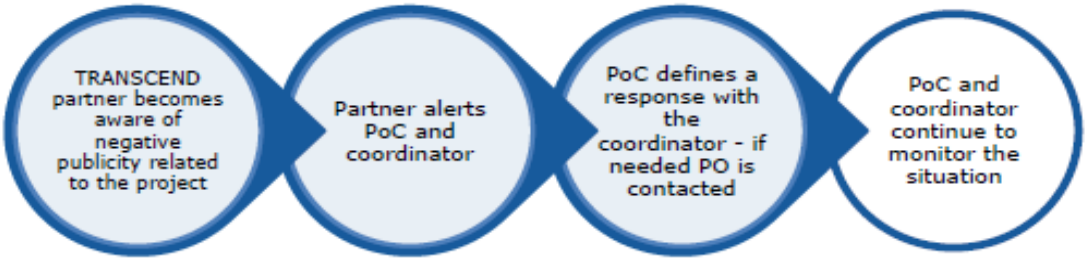


Figure 3 Scenario 2

This is important to end the deliverable by saying that this file is meant to be a dynamic document. If needed, the European Organisation for Security might proceed with updating it.

5

Figure 9: Screenshot of the TRANSCEND Crisis Communication Plan

7.7 Annex 7 - Dissemination log

WEBSITE

METRICS Last update date

METRIC	#
Users overview	
No of downloads per week (deliverables, etc.)	
Overall traffic	
Time on site	
Page visits	
News vs Returning	

Table 20: Metrics for the TRANSCEND Website

Workshops

METRICS

METRIC	#	
No of workshops		
No of participants/workshop		
Workshop n*1		(to target xx-yy ppl)
Workshop n*2		(to target xx-yy ppl)
Workshop n*X		(to target xx-yy ppl)

Table 21: Metrics for the Workshops

Social Media

METRICS

Twitter

Date of the last update

METRIC	#
No of followers (on the XX.XX.202X)	
No of Tweets (on the XX.XX.202X)	
No of Tweet impressions (on the XX.XX.202X)	
Profile Visits (on the XX.XX.202X)	

LinkedIn

Date of the last update

METRIC	#

No of followers	
No of posts	
No of posts impressions	
Profile visits	

Table 22: Metrics for the Social Media

Publications

METRICS

METRIC	#
No of publications:	
Technical journal	
Scientific journal	
Academic journal	
Magazine or newspaper	

PARTNERS	TRI IE	TNO	FhG	EOS	Efus	AutRC	PRIO	CfAll	TRI UK	TOTAL
No of publications:										
Technical journal										
Scientific journal										
Academic journal										
Magazine or newspaper										
Other										

Table 23: Metrics for the Publications

Newsletter

METRICS DATE

METRIC	#
No of subscriptions	
(from Dissemination table)	

DATE

METRIC	#
No of subscriptions	

Table 24: Metrics for the Newsletter

7.8 Annex 8 – Dissemination monitoring spreadsheet

Guidelines - PLEASE READ

Collecting the information in this spreadsheet is **mandatory for EC reporting.** The monitoring spreadsheet has a sheet for dissemination activities, one for communication activities and one for publications. Please make sure you record your activities in the right sheet and that you include the right information in the relevant columns. Each sheet has been adapted from the tables in the EC reporting template (see screenshots below) in order to collect all the information required by the EC and consistently. **PLEASE DO NOT EDIT THE HEADINGS OF THE COLUMNS**.

PLEASE DO NOT EDIT THE DROPDOWN LISTS (last sheet)

Please use the **dropdown menus** whenever indicated in the headings of the columns. These categories have been predefined by the EC and must not be changed.

Read column headings carefully before filling in, as in most cases they include some additional guidelines regarding the type of information that is required.

For each activity, please include as much information as possible (fill in as many columns as you can)

Please mark all the target audiences that apply (target audiences are pre-defined by the EC).

For publications: please fill in details for **ALL columns** that are relevant.

Publications must be written within the context of the project and must contain the following EU acknowledgement and disclaimer: Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them.

Dissemination activities

Continuous Reporting (Dissemination screen) — List the dissemination activities carried out in the context of the project. Include dissemination activities mentioned in the proposal and new ones.

Dissemination Activity Name	What? Type of dissemination activity	Who? Target audience *(Choose one or more items)*	Why? *(max 200 characters)*	Status
[insert activity name]	/Conferences/ /Education and training events/ /Meetings/ /Clustering activities/ /Collaboration with EU-funded projects/ /Other scientific collaboration/ /Other/	/Industry,business partners/ /Investors/ /EU institutions/ /Policy-makers and authorities, international/ /Policy-makers and authorities, national/ /Policy-makers and authorities, regional or local/ /Civil society, international/ /Civil society,national, regional or local/ /Public/ /Standardization bodies/ /Scientists/ /Innovators/ /Specific end-user communities/ /Education/training organization/learners/ /Other/	[insert description of the objective(s) with reference to a specific project output]	/Delivered/ /Cancelled/ /Postponed/ /Ongoing/

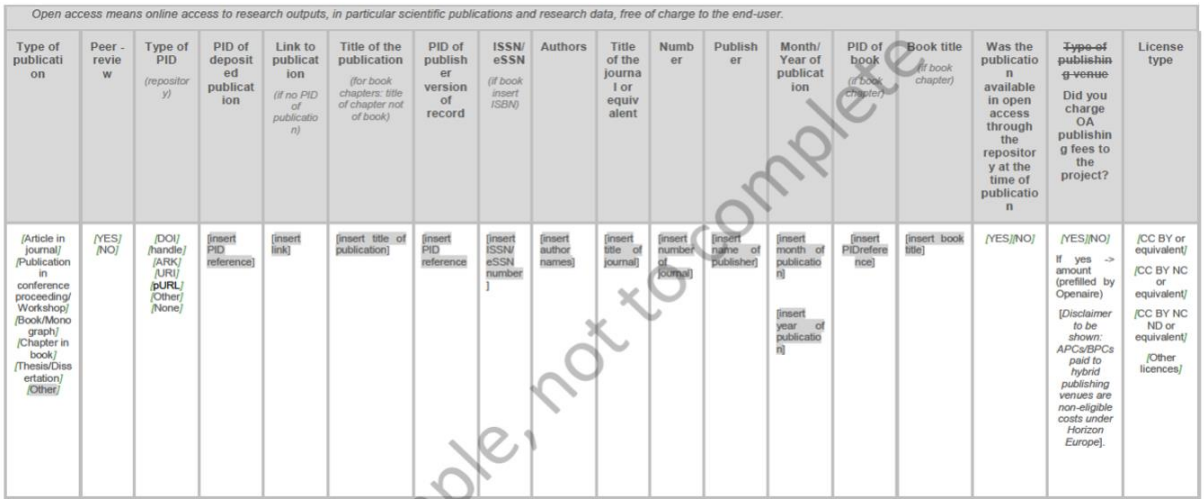
Communication activities

Communication activities

Continuous Reporting (Communication screen) — List the communication activities carried out in the context of the project. Use the same labels used in your DEC plan.

Communication Activity Name	Description	Who? Target audience *(Choose one or more items)*	How? Communication channel *(Choose one or more items)*	Outcome	Status
[insert communication name]	[insert description of implemented communication activity]	/Industry, business partners/ /Innovators/ /Investors/ /EU institutions/ /National authorities/ /Regional authorities/ /Local authorities/ /Civil society/ /Citizens/ /Research communities/ /Specific user communities or applications/ /International organization (UN body,OECD etc)/	/Website/ /Social media/ /Print materials (brochure, leaflet, posters, stickers, banners etc)/ /Press release/ /Media article/ /Newsletter/ /Interview/ /Video/ /TV/Radio campaign/ /Event (conference, meeting, workshop, internet debate, round table, group discussion etc)/ /Exhibition/ /Other/	[insert key performance indicators]	/Delivered/ /Cancelled/ /Postponed/ /Ongoing/

Example, not to be implemented



Open access means online access to research outputs, in particular scientific publications and research data, free of charge to the end-user.

Type of publication	Peer-review	Type of PID (repository)	PID of deposited publication	Link to publication (if no PID of publication)	Title of the publication (for book chapters: title of chapter not of book)	PID of publisher version of record	ISSN/ eSSN (if book insert ISBN)	Authors	Title of the journal or equivalent	Number	Publisher	Month/ Year of publication	PID of book (if book chapter)	Book title (if book chapter)	Was the publication available in open access through the repository at the time of publication	~~Type of publishing venue~~ Did you charge OA publishing fees to the project?	License type
[Article in journal/ /Publication in conference proceeding/ Workshop/ /Book/Monograph/ /Chapter in book/ /Thesis/Dissertation/ /Other/	/YES/ /NO/	/DOI/ /handle/ /ARK/ /URI/ /pURL/ /Other/ /None/	[insert PID reference]	[insert link]	[insert title of publication]	[insert PID reference	[insert ISSN/ eSSN number]	[insert author names]	[insert title of journal]	[insert number of journal]	[insert name of publisher]	[insert month of publication] [insert year of publication]	[insert PIDreference]	[insert book title]	/YES/NO/	/YES/NO/ If yes -> amount (prefilled by Openaire) [Disclaimer to be shown: APCs/BPCs paid to hybrid publishing venues are non-eligible costs under Horizon Europe].	/CC BY or equivalent/ /CC BY NC or equivalent/ /CC BY NC ND or equivalent/ /Other licences/

Sample, not to complete

Figure 10: Guideline for Communications and Dissemination Activities and Publications (extracted from the AGA and Horizon Programme Guidelines)

Dissemination activities - - - > scroll right for audiences

Partner (SELECT FROM DROPDOWN MENU)	Activity	Description (including objective/s with reference to a specific project output)	Type of activity (SELECT FROM DROPDOWN MENU)	Date	Outcome (INDICATE KPI from dissemination plan)	Status (SELECT FROM DROPDOWN MENU)

Target audiences (MARK ALL THAT APPLY)													
Industry, business partners	Investors	EU institutions	Policymakers and authorities (INTERNATIONAL)	Policymakers and authorities (NATIONAL)	Policymakers and authorities (REGIONAL OR LOCAL)	Civil society (INTERNATIONAL)	Civil society (NATIONAL, REGIONAL OR LOCAL)	Public	Standardisation bodies	Scientists (& research communities)	Specific end-user communities	Education/training organisation/ learners	Other

Table 25: Template Dissemination activities retrieved from the monitoring spreadsheet

Communication activities - - - > scroll right for audiences

Partner (SELECT FROM DROPDOWN MENU)	Activity	Description	Channel used (SELECT FROM DROPDOWN MENU)	Date	Outcome (INDICATE KPI from dissemination plan)	Status (SELECT FROM DROPDOWN MENU)

Table 26: Template Communication Activities retrieved from the monitoring spreadsheet

Media coverage - press/blog articles				
Date (DD/MM/YY)	**News outlet**	**Country**	**Link**	**Mitigation / follow up**

Table 27: Template Media coverage retrieved from the monitoring spreadsheet

Publications																		
Partner (SELECT FROM DROPDOWN MENU)	Type of publication (SELECT FROM DROPDOWN MENU)	Peer-review (MARK YES OR NO)	Type of PID (repository) - SELECT FROM DROPDOWN MENU	PID of deposited publication (INSERT PID REFERENCE)	Link to publication (if no PID of publication)	Title of the publication (for book chapters: title of chapter not of book)	PID of publisher version of record	ISSN or Essn	Authors	Title of the journal or equivalent	Number	Publisher	Month/ Year of publication	PID of book (if book chapter)	Book title (if book chapter)	Was the publication available in open access through the repository at the time of publication (MARK YES OR NO)	Did you charge OA publishing fees to the project? (MARK YES OR NO + AMOUNT SPENT IF YES)	License type (SELECT FROM DROPDOWN MENU)

Table 28 Template from Publications retrieved from the monitoring spreadsheet