Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OCCTET

Open Source Compliance Comprehensive tools and resources designed to simplify and streamline the CRA compliance process for SME, allowing them to tackle the complexities of OSS compliance.

Project Title: Open Source Compliance Comprehensive tools and resources designed to simplify and streamline the CRA compliance process for SME, allowing them to tackle the complexities of OSS compliance.
Project Acronym: OCCTET
Grant Agreement / Contract No.: 101190474
Program: DIGITAL Europe Programme; DIGITAL-ECCC-2024-DEPLOY-CYBER-06
Instrument: DIGITAL JU SME Support Action
Granting Authority: European Cybersecurity Industrial, Technology and Research Competence Centre
Project Start Date: 1 November 2024
Project Duration: 24 months

Deliverable Number: D5.1
Deliverable Title: Communication, Dissemination and Outreach Strategy
Deliverable Type (DOA): R — Document, report
Deliverable Type (content): Document identifying key audiences, events, messages, stakeholders and activities that will be used to gather requirements, promote tools and enhance uptake throughout project duration and beyond. Sets out KPIs and impact measures.
Work Package: WP5 – Dissemination - Communication - Outreach and Impact
Task Number(s): T5.1- Communication and dissemination
Dissemination Level: PU – Public
Due Date (DoA): 30 April 2025
Actual Submission Date: 30 April 2025
Version: 1.1 (PR1 Revision)

Lead Beneficiary: DSME- Digital SME Alliance
Main Author(s): Davide Iaccarino - DSME
Contributing Partner(s): -
Reviewer: ECL - Eclipse Foundation Europe

Document History

Version	Date	Issued By	Status	Comments
0.1	19-03-2025	DSME	Draft	Initial draft of D5.1
0.2	29-04-2025	ECL	Review	QA review
1.0	30-04-2025	ECL	Final	Release V1.0
1.1	18-02-2026	ECL	Final	Addressing the recommendations from the Review Report

Executive Summary

This document, Deliverable D5.1, outlines the "Communication, Dissemination and Outreach Strategy" for the OCCTET project. The core objective is to raise awareness and drive the adoption of the toolkit, targeting at least 1,000 active users within the 24-month project duration.

The strategy is executed in three phases:

1. **Pre-launch (M1–M8):** Branding, anticipation building, and needs analysis workshops.
2. **Post-Launch (M9–M20):** Active promotion through webinars, training, social media, and industry events.
3. **Sustainability (M20–M24):** Ensuring long-term use and maintenance via knowledge transfer.

Key audiences include SMEs, Open-Source Developers, Regulatory Authorities, and European Digital Innovation Hubs (EDIHs). Communication leverages a multi-channel approach (website, LinkedIn, GitHub, events) tailored with key messages on "Simplifying CRA compliance" and "Open Source Security."

Success is monitored via Key Performance Indicators (KPIs).

Keywords: Cyber Resilience Act (CRA), SMEs, FOSS, Open Source Compliance, Dissemination Strategy, communication, events.

Table of contents

1 Introduction

This document establishes the Dissemination, Communication & Outreach Strategy Plan for the OCCTET project. It outlines the objectives of dissemination and communication while addressing the specific needs of the different Work Packages in terms of outreach and engagement. The strategy identifies the target audiences and the communication tools and channels to effectively reach them. Additionally, it provides an operational plan for implementing communication activities and an overview of impact measurement and KPI monitoring.

The OCCTET project aims to empower SMEs by simplifying compliance with the Cyber Resilience Act (CRA) through a cost-effective and user-friendly toolkit. By leveraging open-source tools and promoting community collaboration, OCCTET addresses critical aspects such as dependency management, risk management, and open-source security. The minimalist yet robust approach ensures free and accurate CRA compliance, making it accessible to SMEs across Europe. Through its dissemination efforts, the project highlights key messages of simplifying compliance, empowering SMEs, and promoting a sustainable, open-source solution for managing cybersecurity risks. These efforts aim to position OCCTET as a leading resource in advancing SME compliance and enhancing cybersecurity resilience across the EU.

1.1 Purpose and Scope of this document

The purpose of this document is to align OCCTET's overall goals and strategy with the dissemination and communication activities. Thus, this Plan introduces the project's dissemination and communication strategy and its implementation plan to be used by the consortium to ensure the high visibility, accessibility and promotion of the project and its results, with the ultimate goal of increasing participation by key stakeholders in the design phase and increasing uptake of the resulting toolkit. In addition, it gives an overview of the main communication tools and channels, as well as target audiences to be reached. Furthermore, this deliverable provides an approach and strategic planning for all future communication and engagement actions, including impact and KPI monitoring for these activities.

This Plan is a comprehensive and living document, which will be reviewed on a rolling basis. Should some of the initially planned communication performance indicators not be on the right track, actions to mitigate the issues will be carried out, even if they deviate from the initial planning provided hereby.

2 Dissemination and Communication Strategy Approach

The dissemination strategy will focus on establishing a strong identity for OCCTET and setting up the methodology, tools and channels in order to raise OCCTET's key stakeholder group's awareness about the project as well as their interest in the project's results.

The primary objective is to raise awareness about the project and generate interest in its results, particularly the open-source toolkit designed for Cyber Resilience Act (CRA) compliance. The overall goal of the communication and dissemination activities is to reach at least 1,000 active users of the toolkit by the end of the project.

To achieve this, the strategy will target SMEs, open-source developers, policymakers, and cybersecurity authorities through a combination of activities, such as webinars, workshops, newsletters, and online campaigns. Key performance indicators (KPIs) include 10,000 website visits, 1,000 toolkit downloads, and active engagement through social media and GitHub platforms. By aligning these efforts with the project's objectives, the dissemination strategy will ensure OCCTET's results are widely adopted, and its impact maximised across Europe.

2.1 Communication and Dissemination Objectives

In order to achieve this ambitious goal, the implementation of the project activities will go hand-in-hand with a communication and dissemination plan. The Plan will thus be aligned with the strategic importance of the project. The overall goal of the OCCTET communication and engagement activities is to to raise awareness about the project's key results, including the development of a free, open-source toolkit for Cyber Resilience Act (CRA) compliance, practical guidance for SMEs on dependency and risk management, and the promotion of open-source security practices. These results are designed to simplify CRA compliance for SMEs, reduce costs, and empower businesses to adopt effective cybersecurity practices. The communication and dissemination activities will serve the needs of all the Work Packages of the project, throughout the project's duration.

In order to enhance the project's visibility and to maximise its impact in terms of benefits brought to society and economy, the dissemination and communication activities will aim to:

1. Raise awareness about the project;
2. Disseminate all the project's results and achievements;
3. Support the engagement of the project's target audience and relevant stakeholders;
4. Promote the project's activities and regularly inform the project's target audience;
5. Design, produce and distribute adequate communications materials to the identified target groups;
6. Disseminate the knowledge and know-how created by the consortium;
7. Promote the added value of the project for the European society and economy;

8. Ensure the sustainability of the project beyond its lifetime;
9. Organise engaging and informative events;
10. Promote SME-targeted communication regarding the Cyber Resilience Act and compliance tools;

2.2 Contribution of Dissemination and Communication to the Project's Results

The Dissemination, Communication & Outreach strategy of the OCCTET project ensures that project results are not only widely disseminated but also effectively adopted by SMEs and other key stakeholders. By aligning specific communication actions with the objectives of each Work Package, the strategy supports the project's overarching goals of increasing SME compliance with the Cyber Resilience Act, fostering collaboration, and advancing the European cybersecurity posture. This approach emphasizes tailored messaging, stakeholder engagement, and the effective use of both digital and traditional communication channels to maximise the project's visibility and impact.

The table below outlines the expected results of each WP and the corresponding communication and dissemination contributions:

Table 1 - Contribution of Dissemination and Communication to the Project's Results

Work Package	Expected Results	Communication and Dissemination Contribution	Tools/Channels
WP1	• To ensure timely, high-quality delivery of project results through administrative, technical, and financial coordination. • To foster alignment with European policies for cybersecurity and SME resilience.	Promotion of all the public results delivered; Highlight the project's alignment with EU policies in all communications to foster trust and engagement.	Project Website, Press Releases, Social Media, Newsletters/Emails

WP2	• To develop checklists and guidelines for CRA compliance tailored to SMEs. • To map challenges and requirements faced by SMEs for CRA adherence.	Organise Q&A sessions and virtual consultations to engage SMEs and gather feedback.	In-Person Event and Webinars, Email Campaigns, Website Articles
WP3	• Deliver FOSS tools that simplify CRA compliance. • Provide resources for automating SBOM creation and vulnerability assessments.	Host live webinars and tutorials to demonstrate the tools' utility. Publish case studies and user guides on project and partner platforms. Collaborate with digital innovation hubs for localised demonstrations.	Webinars and Tutorials, Case Studies and User Guides
WP4	• Validate the tools and procedures using SME-led pilot projects • Capture insights and refine tools based on practical application	Develop and share success stories from SMEs through blogs, newsletters, and video testimonials. Highlight lessons learned and actionable insights at industry events and conferences.	Industry Events, Conferences, Blogs and Newsletters

WP5	• Raise awareness of OCCTET results across Europe. • Engage stakeholders including SMEs, policymakers, and FOSS communities. • Build relationships with related EU projects and initiatives.	Implement a comprehensive outreach plan, including press releases, webinars, and newsletters. Engage SMEs and policymakers through targeted campaigns and events. Promote project results in industry publications and social media campaigns.	

The strategy not only amplifies the visibility of the project's results but also creates a sustainable framework for continued use and impact beyond the project's duration. Through targeted and coordinated efforts, OCCTET's dissemination actions will contribute to SME resilience, promote cybersecurity best practices, and contribute to the broader goals of the CRA.

2.3 Communication Methodology

The communication methodology for the OCCTET project aims at ensuring that project results are effectively disseminated, widely adopted and sustained by SMEs and other key stakeholders. By using a multi-channel approach and targeted messaging, the methodology facilitates continuous engagement throughout the project lifecycle, ensuring that the outputs meet the needs of the SME community, FOSS developers, policy makers and other stakeholders. The strategy is structured around clear objectives, specific communication actions, and ongoing evaluation to adapt to stakeholder feedback.

Stakeholder Mapping and Targeting: a key element of the communication strategy is identifying and engaging the right stakeholders. The primary focus is on SMEs, which form the core audience for OCCTET's tools and resources, as they are directly impacted by the Cyber Resilience Act and the need for compliance. DSME's extensive network of SMEs across Europe will be leveraged to ensure the message reaches the right audience. Moreover, the strategy targets FOSS communities, industry leaders, and policymakers who influence or are directly involved in cybersecurity standards and regulations. These stakeholders will be reached through a variety of communication channels to ensure diverse and widespread impact.

Key Messaging and Content Strategy: clear and consistent messaging is essential to convey the importance and impact of the OCCTET tools. The core message revolves around the

facilitation of CRA compliance for SMEs, the security of open-source software components, and the broader goals of the EU's cybersecurity strategy. For SMEs, the messaging emphasizes how OCCTET tools simplify and automate the compliance process, reducing time and costs. For FOSS communities, the focus is on securing open-source software components, managing vulnerabilities, and contributing to the EU's digital sovereignty. The content strategy includes different formats, such as written articles, website posts, infographics, knowledge-sharing videos, and case studies, all tailored to the specific needs of each stakeholder group. Regular newsletters and project updates will also keep stakeholders informed about new developments, milestones, and achievements.

Communication Channels and Tools: a wide array of communication channels will be employed to reach stakeholders effectively. Digital platforms will serve as the primary means of outreach. The project website will act as a central hub for news, resources, and tool downloads. Social media channels such as LinkedIn and YouTube will be used to share updates, event promotions, and thought leadership content. Email campaigns will provide stakeholders with regular newsletters that highlight key results, upcoming events, and success stories. In addition to digital channels, traditional methods such as conferences, workshops and roundtables will be used to engage stakeholders in person and provide more in-depth discussions. Participation in EU and international cybersecurity events will offer opportunities to present OCCTET's tools and results to a wider audience. Press releases will also be distributed to relevant media outlets to maximise project visibility.

Engagement and Interaction: the communication strategy is designed to promote two-way communication, ensuring that the project stays responsive and relevant to stakeholder needs. Regular feedback mechanisms, including surveys, polls, and direct consultations, will be implemented to gather input from SMEs and other key stakeholders. This will help shape the development of OCCTET's tools and ensure that the project's outputs are relevant and useful. The project will also engage SMEs directly in the testing and validation of tools, using their real-world experiences to refine and improve the resources. Community engagement will be a central part of the strategy. A project website will be created to foster interaction among stakeholders, where SMEs, FOSS developers, and policymakers can share their experiences, ask questions, and collaborate on solutions. This community-driven approach will help maintain long-term engagement and promote the sustained use of OCCTET tools beyond the project's duration.

Monitoring and Evaluation: to ensure the effectiveness of communication efforts, key performance indicators (KPIs) have been established. These include metrics such as website traffic, social media reach, email open rates, and engagement levels in webinars and events. The project will also track the number of tool downloads, the extent of stakeholder participation, and the adoption rates of OCCTET's solutions among SMEs. Feedback from stakeholders will be regularly collected through surveys, interviews, and direct engagement to evaluate the impact of the communication activities and adjust the strategy where necessary.

Sustainability and Long-Term Impact: the sustainability of the project's communication efforts is crucial for ensuring that OCCTET's tools continue to be useful after the project ends. The communication strategy will establish partnerships with key stakeholders, such as Digital

Innovation Hubs, SME networks, and FOSS communities, to maintain ongoing support for the tools. Additionally, a long-term communication plan will be developed to keep stakeholders engaged, ensuring that the project's outcomes remain relevant and continue to support SMEs in meeting CRA compliance requirements.

2.4 Communication Adjusted to the Project's Work Plan

Through the project life cycle, different communication means, and channels will be used, depending on the specific stakeholders to be targeted at that stage of the project, as well as the main project results and messages to be promoted. Therefore the project is divided into three main periods (phases), which are linked to different communication and engagement strategies, channels and messages used in each stage.

The **launch of the OCCTET toolkit** will mark the transition from early awareness-building and needs analysis to active engagement with end-users. The table below provides an overview of communication and dissemination activities across all project phases, highlighting how each stage supports the introduction, adoption, and long-term impact of the toolkit.

Table 2 - Communication Strategy Through Different Phases of the Project

Communication Strategy Through Different Phases of the Project	
Pre-launch (M1 – M8) – focuses on engaging a potential user base of SMEs and open-source developers while leveraging on key multipliers including SME organisations, public sector bodies, and European Digital Innovation hubs. During this stage, targeted outreach will invite SMEs to participate in co-design and needs assessment activities, ensuring that the toolkit reflects real compliance challenges and user requirements.	Aim: to engage SMEs, facilitate use-case development for the toolkit, and promote its adoption Stakeholders: national and European SME organisation, European Digital Innovation Hubs, NCCs, Cyber Authorities Communication channels & tools: crafted mailings, events and workshops, project presentations, social media, website. The website will serve as the central hub for the project and end-users will be able to subscribe to the OCCTET newsletter that will gather all relevant news regarding the development of the project. Communication themes: supporting SMEs with digital challenges; promoting cyber skills and compliance; potential synergies. This stage is characterised by creating anticipation for the OCCTET toolkit as a much-needed solution. The key messages that will be disseminated through OCCTET's social media channels and its website will focus on the urgency of CRA compliance, positioning OCCTET as an essential tool. By engaging stakeholders in this early process through needs assessments, co-design activities and targeted

	storytelling, such as case studies and training that can be included in webinars and workshops, the strategy will ensure that a strong user base is already waiting for the toolkit at launch. This will also be reinforced by the 100 SMEs who will commit to the early-access wishilist.
Post Launch (M9 – M20) – aims to promote the tool to European companies and engage the open-source community for adoption, continuity, and user feedback. Actions include a centralised information hub, dissemination activities, and use of social and traditional media, targeting the same audience.	Aim: to promote the tool across Europe and encourage adoption and feedback from the SMEs and open-source community. Stakeholders: National and European Associations to be identified in each country covered by project partners, Cyber Authorities, NCCs, Legal Associations. Communication channels & tools: social media (Linkedin, Substack), media (journals and magazines, industry conferences and in person events. Communication themes: raising awareness regarding the tool, promoting open source adoption and community engagement, ensuring continuity and user feedback for project improvement. During the post-launch phase, targeted engagement with EDIHs and NCCs will be strengthened to leverage their role as regional multipliers. By integrating OCCTET dissemination activities within their existing SME support frameworks, the project aims to broaden outreach beyond the consortium's direct networks and ensure sectoral and geographical representativeness.
Post Project (M20 – M24) - **ensures** the software's continuity by maintaining access points and the repository for ongoing use and contributions from the open-source community	Aim: to ensure the project's outputs' continuity by maintaining access to the software and supporting open-source contributions. The Toolkit will be accessible through the official OCCTET website that will be updated in time as SMEs, at this point, will be regular users

	of the software. Each consortium partner will ensure that the website and the toolkit will be reachable through their own company channels. Depending on partners, more activities will be set out in order to keep momentum with the Toolkit in post-launch discussions. Stakeholders: SMEs and Companies, organisations seeking ongoing access to the toolkit Communication channels & tools: industry events partners may be attending post-project Communication themes: ensuring long-term accessibility of the toolkit, supporting open-source contributions and collaboration

3 Target Audiences

The following table presents the targeted dissemination approach of OCCTET by distinguishing stakeholder segments according to their role within the Cyber Resilience Act ecosystem. Rather than addressing SMEs as a homogeneous audience, the project differentiates between digital product manufacturers, open-source developers, cybersecurity adopters, ecosystem multipliers and policy stakeholders. For each segment, specific pain points, expectations and tailored key messages are identified. This structured segmentation ensures that dissemination efforts are proportionate to the regulatory responsibilities, technical maturity and operational context of each stakeholder group.

Table 3 - Target Audiences

Target Audiences	Composition	Paint Points	Needs and Expectations	Key Messages
Digital Product SMEs	SMEs developing, manufacturing or integrating digital products falling under the scope of the Cyber Resilience Act (software vendors, IoT manufacturers, SaaS providers, embedded systems developers).	Uncertainty about product classification and CRA liability Limited visibility over third-party software components Increased compliance documentation burden Difficulty aligning legal and technical teams	.Clear mapping between product type and CRA obligations Practical SBOM and vulnerability management tools Guidance on conformity assessment pathways Integration of compliance into product lifecycle processes	“Understand your product type and CRA obligations” “Integrate compliance into your product lifecycle!” “Reduce supply chain risk without increasing operational burdens”

Open-Source Developers & Communities	Open Source Developers OSS maintainers Technical contributors operating within SMEs Technical contributors to software supply chain Developers working with Software Bill of Materials (SBOM) and vulnerability management tools.	Uncertainty on how CRA applies to open-source contributions Risk of being unintentionally considered a manufacturer Lack of structured SBOM workflows Concern that compliance may hinder innovation	Clarification of roles under CRA Integration of compliance into CI/CD pipelines Alignment with open-source best practices Community-oriented security approaches	“Clarify your role under the CRA” “Embed compliance checks into your development workflow” “Strengthen open-source transparency without limiting innovation”
Cybersecurity & Regulatory Authorities	National cybersecurity agencies responsible for overseeing CRA implementation. European cybersecurity regulatory	Need for practical CRA tools for SMEs Limited regulatory interpretation capacity Difficulty scaling compliance	Ready-to-use compliance toolkit Training materials for SME onboarding Structured guidance	“Integrate OCCTET into your SME support services” “Scale CRA awareness through your regional network”

	bodies, including ENISA and national CERTs.	support across sectors	adaptable to regional contexts	"Provide structured compliance pathways to SMEs"
SMEs Adopting Cybersecurity Practices	SMEs integrating digital tools into operations but not directly developing software products.	Limited in-house cybersecurity expertise Difficulty translating regulatory language into practical steps Resource constraints Uncertainty about indirect CRA implications	Simplified compliance guidance Step-by-step onboarding support Access to trusted intermediaries Clear distinction between direct and indirect obligations	"Pratical CRA guidance tailored for SMEs" "Accessible tools supported by trusted partners" "Understand what applies to your business and what does not"
Strategic Partners & Related EU Projects	EU-funded cybersecurity and digital resilience projects Standardisation Initiatives Research organisations Open-source foundations	Risk of fragmentation across EU-funded compliance initiatives Overlapping dissemination efforts Limited interoperability between tools	Alignment of CRA-related communication and terminology Cross-project visibility and knowledge exchange Coordinated outreach toward shared SME audiences	"Align CRA compliance efforts across EU initiatives" "Avoid fragmentation through coordinated open-source approaches"

		and methodologies		"Strengthen EU digital resilience through collaboration"
European Digital Innovation Hubs (EDIHs)	One-stop shops assisting SMEs and the public sector with digital transformation and cybersecurity compliance Hubs focusing on cybersecurity training and support for CRA compliance Regional and national EDIHs acting as multipliers for OCCTET's toolkit.	SMEs assisted by EDIHs may lack awareness of CRA and its impact Need for tangible, easy-to-adopt tools for compliance Limited direct resources to support regulatory compliance efforts	Available compliance toolkits to guide SMEs Workshops and training that integrate with EDIHs offerings. Clear communication materials to help educate SMEs on CRA	"Integrate OCCTET into your SME support portfolio to address CRA compliance!" "Offer practical SBOM and supply chain guidance through OCCTET!" "Scale compliance awareness across sectors through your regional network!"
National Competence Centres (NCCs)	EU-funded centres supporting research, innovation, and industry collaboration in cybersecurity.	Need to support SMEs with cutting-edge cybersecurity knowledge Difficulty ensuring	Access to open-source cybersecurity tools tailored for SMEs. Opportunities to contribute	"Leverage OCCTET to translate cybersecurity policy into operational SME tools."

	Organisations helping businesses adopt secure digital solutions and best practices Key actors in facilitating SME access to cybersecurity expertise and funding	research findings translate into practical solutions Limited collaboration with open-source communities	expertise in shaping compliance solutions. Training materials and best practices for scaling cybersecurity adoption.	"Enhance national resilience by scaling structured CRA readiness among SMEs." "Support national CRA implementation through industry-aligned compliance resources." "Strengthen SME cybersecurity maturity with open-source assurance mechanisms."

The segmentation outlined above is implemented through clearly differentiated dissemination channels and event participation aligned with each stakeholder profile. For open.source developers and FOSS communities, outreach prioritises participation in major open-source and compliance-focused events such as FOSDEM and Code & Compliance, organised by the Eclipse Foundation. In addition, OCCTET will explore possibilities to engage through collaborative platforms such as GitHub and GitLab repositories, and will use dissemination channels, such as OFE Community mailing list to further promote the key outputs. Engagement also includes technical webinars dedicated to SBOM generation, vulnerability management workflows, and integration of compliance checks into CI/CD pipelines, as well as interaction within developer mailing lists and open -source fora.

For digital product manufacturers and ICT integrators, dissemination is also conducted through cybersecurity and industry oriented events such as Cybersec Europe, Infosecurity Europe, and through annual events such as the DIGITAL SME Summit. These channels allow OCCTET to address product liability, conformity assessment pathways and supply chain risk management in a business-focused context. Additional outreach is conducted through SME association networks, including SMEUnited, CEA-PME and the European DIGITAL SME Alliance, ensuring direct access to product-oriented SMEs.

SMEs adopting cybersecurity practices without internal development capacity are primarily

engaged through EDIHs, NCCS, and regional innovation networks. Targeted briefings, joint workshops and integration of OCCTET material into EDIH service portfolios ensure that compliance guidance remains accessible, practical, and geographically representative.

EDIHs are engaged as multipliers by positioning OCCTET as a ready-to-use compliance support instrument within their SME advisory services. NCCs are engaged through policy-aligned briefings and cybersecurity coordination events to ensure that OCCTET contributes to national-level CRA implementation efforts and SME capacity-building strategies.

Through this structured and segment-specific approach, dissemination activities are tailored to the regulatory responsibilities, technical maturity and operational realities of each stakeholder category, thereby maximising relevance and adoption potential. Meanwhile, horizontal dissemination instruments - including the project website, periodic newsletters, social media channels, etc. - will also be used towards all audiences (as described in the next Chapters), and will ensure sustained visibility and long-term accessibility of project outputs.

3.1 SWOT Analysis

A structured SWOT analysis has been developed for OCCTET to provide a clear overview of the project's internal strengths and weaknesses, as well as the external opportunities and threats present in the regulatory and market environment. This analysis serves as a basis for the communication and dissemination strategy by highlighting areas where key messages can leverage existing strengths and opportunities while addressing weaknesses and mitigating risks.

The analysis identifies several strengths, including a strong consortium with deep expertise in cybersecurity, FOSS compliance, and SME outreach; alignment with EU priorities such as the Cyber Resilience Act; a comprehensive toolkit designed to address critical challenges faced by SMEs, and an open-source approach that ensures accessibility and fosters collaboration. Additionally, the SME network available through the European DIGITAL SME Alliance represents a significant asset for targeted dissemination.

On the other hand, certain weaknesses have been noted, such as limited awareness among SMEs regarding the complexity and importance of CRA compliance, constraints imposed by the project timeline, reliance on the stakeholder willingness to adopt new tools, and variability in technical expertise among SMEs. External opportunities include increasing awareness of cybersecurity compliance, potential partnerships with Digital Innovation Hubs and industry leaders. Potential threats include the risk of regulatory changes affecting CRA compliance requirements, limited resources among SMEs that may lower the level of implementation, competition from other compliance tools, and possible resistance from stakeholders unfamiliar with open-source solutions.

The following table expands on OCCTET's SWOT analysis by identifying strategic actions to leverage strengths, address weaknesses, exploit opportunities, and mitigate potential threats. This approach ensures that the project maximises its impact, enhances stakeholder engagement, and proactively adapts to challenges, securing the long-term success and adoption of its results:

Table 4 - SWOT Analysis

Category	Key Points	Strategic Actions
Strengths	**Strong consortium with expertise in cybersecurity, FOSS compliance, and SME outreach.**	Leverage partner networks to ensure wide adoption of OCCTET tools and engage in joint dissemination efforts at key industry events and policymaking discussions.
Strengths	**Alignment with EU priorities, including the Cyber Resilience**	Highlight alignment in all communications and policy engagement efforts to secure credibility and potential

	Act and the European Cybersecurity Strategy.	funding for sustainability beyond the project's duration.
Strengths	**Comprehensive toolkit designed to address critical challenges faced by SMEs.**	Ensure that the toolkit is user-friendly, well-documented, and extensively tested to maximise adoption and usability. Offer training sessions and clear guidelines.
Strengths	**Open-source approach ensures accessibility and promotes collaboration within FOSS communities.**	Engage actively with open-source communities through GitHub, open discussions, and collaborative development to encourage contributions and long-term sustainability.
Strengths	**Leveraging DSME's extensive SME network for targeted dissemination.**	Use DSME's communication channels, mailing lists, and events to maximise SME engagement and build an initial user base before the toolkit launch.
Weaknesses	**Limited awareness among SMEs about the complexity and importance of CRA compliance.**	Develop targeted awareness campaigns, workshops, and explainer materials tailored for non-technical SME audiences. Partner with industry bodies to enhance reach.
Weaknesses	**Project timeline may constrain outreach and engagement efforts.**	Prioritise high-impact activities in the first 12 months (e.g., early adopters, social media engagement, and multiplier partnerships) to accelerate traction before the final phase.
Weaknesses	**Dependence on stakeholder willingness to adopt new tools and practices.**	Offer incentives for early adopters (e.g., recognition, free training, case study features) and demonstrate clear business benefits to encourage adoption.
Weaknesses	**Variability in SME technical expertise may challenge the adoption of advanced tools.**	Ensure toolkit accessibility by providing tiered compliance solutions (basic vs. advanced), and develop intuitive interfaces with clear step-by-step guidance.
Opportunities	**Rising awareness about the importance of compliance with cybersecurity standards.**	Position OCCTET as a go-to resource for SMEs and open-source developers, ensuring continuous engagement through thought leadership content and expert insights.

Opportunities	**Potential for partnerships with Digital Innovation Hubs, policymakers, and industry leaders to amplify project impact.**	Strengthen partnerships with EDIHs and cybersecurity networks to integrate OCCTET's toolkit into their SME support initiatives, ensuring long-term sustainability.
Opportunities	**Establishing OCCTET as a cornerstone for CRA compliance in the European Union.**	Build credibility through endorsements from EU institutions, national cybersecurity bodies, and SME associations. Publish impact reports to showcase adoption rates and effectiveness.
Threats	**Risk of regulatory changes that may alter CRA compliance requirements.**	Maintain flexibility in toolkit development by designing modular features that can be adapted based on evolving CRA guidelines and industry standards.
Threats	**Limited resources among SMEs may diminish their ability to implement solutions, despite their relevance.**	Emphasise cost-effectiveness in messaging, offer free resources, and collaborate with policymakers to advocate for SME-friendly support programs.
Threats	**Competition from other compliance tools or initiatives could fragment stakeholder attention.**	Highlight OCCTET's unique value proposition (open-source, SME-focused, community-driven) and actively participate in discussions to differentiate from commercial alternatives.
Threats	**Potential resistance from stakeholders unfamiliar with open-source solutions.**	Educate policymakers and SMEs on the security benefits of open-source tools, leveraging case studies and expert advocacy to dispel misconceptions.

4 Dissemination, Communication Tools and Channels

All the tools, means and channels for the dissemination of the project results and the interaction with the OCCTET stakeholders are described in this chapter. This includes defining the project's identity, i.e., its values, purpose, visual identity, as well as describing its dissemination channels.

4.1 Project Branding and visual identity

A strong and consistent visual identity is essential for building recognition and trust in OCCTET, The project's branding reflects its core mission of making cybersecurity compliance accessible, transparent, and practical for SMEs and the open-source community.

The OCCTET colour palette, centered around shades of blue, conveys trust, security, and technological reliability, aligning with its role in supporting SMEs with compliance tools and cybersecurity best practices. The selected fonts and templates ensure clarity, professionalism, and consistency across all communication materials, from reports and presentations to the website and social media.

4.1.1 Colour Palette

OCCTET's colour palette has been carefully selected to reflect the project's core values of trust, security, and digital innovation. The dominant shades of blue, ranging from Congress Blue to Denim and Steel Blue, symbolise reliability, professionalism, and technological excellence. These colours are commonly associated with cybersecurity and digital trust, reinforcing OCCTET's mission to provide transparent, open-source compliance solutions for SMEs. The inclusion of these tones ensures strong visual contrast, promoting readability across digital and print materials while maintaining a modern and cohesive aesthetic. This consistent use of colour across OCCTET's branding, website, and communication materials will help establish a recognisable identity in the European cybersecurity landscape.

4.1.2 Logo

The OCCTET logo visually represents the project's mission to facilitate cybersecurity compliance for SMEs. The shield shape symbolises protection and resilience, reinforcing OCCTET's role in supporting businesses as they navigate the requirements of the CRA. The geometric segmentation within the shield conveys structure and collaboration, reflecting the harmonisation of cybersecurity practices across different stakeholders. The blue gradient colour palette is associated with trust, security, and innovation, aligning with OCTET's commitment to providing clear, actionable, and accessible cybersecurity guidance. This modern and professional design will ensure that OCCTET remains visually recognisable and aligned with the European cybersecurity landscape, strengthening its branding in all communications.

4.1.3 Fonts

OCCTET has adopted Aptos Display as its primary font to ensure a modern, professional, and highly readable visual identity. Aptos Display was selected for its clean design, versatility, and accessibility, making it well-suited for both digital and printed materials. Its contemporary style aligns with OCCTET's goal of providing clear and structured communication on cybersecurity compliance for SMEs. The use of a standardised font across all materials promotes brand consistency and recognisability throughout the project.

4.1.4 Template

To maintain a consistent and professional format across all project communications, OCCTET has developed a set of official templates:

- Presentation Template: a structured slide deck for project meetings, webinars, and external engagements, ensuring clarity and uniformity in visual presentations.
- Official Document Template: a standardised format for deliverables, reports, and other official documentation, facilitating coherence and readability across project outputs.

4.2 Communication and Dissemination Channels

In order to successfully attract the target audiences, promote the OCCTET results and activities and engage its stakeholders, OCCTET will be communicating tailored messages

through the most effective channels and tools that are adapted to the stakeholders' needs. To this end, a multi-channel strategy and a blend of communication measures is foreseen, and the main channels planned for the project are presented in this sub-chapter.

4.2.1 OCCTET Website

The OCCTET website content and resources will act as an entry point and as a one stop shop for all information and engagement actions. The chosen domain for the website will be occte.eu. Using the project's name as the website domain name will help solidify OCCTET's stance and will be more easily recognisable by end-users. The website will host surveys for CRA compliance-related needs analyses as well as CRA-related information in order to support and highlight the functionalities of the OCCTET Tool and its importance in the context of the implementation of the Cyber Resilience Act.

The OCCTET website will be developed according to the visibility guidelines of the European Commission, and it will feature a user-friendly interface that will include:

- Interactive homepage with key news and direct links to the main sections on the rest of OCCTET website.
- Registration plug-in providing the possibility to register to OCCTET-related newsletters.
- Toolkit section – one of the core sections of the website which provides a direct link to the Toolkit and code repositories.
- Self-assessment section which will provide end-users with the possibility to assess their posture regarding CRA compliance.
- News & Events: any relevant news / upcoming events linked to the project will be shown here.
- CRA section where users will find SMEs-tailored information regarding the implementation of the Cyber Resilience Act.

To ensure efficiency, scalability, and security, the website has been built using Hugo, a lightweight and high-performance static site generator. This choice enables fast load times, enhanced security, and easy content management, allowing for seamless updates and adaptability throughout the project's lifecycle. The website will continuously evolve to reflect project milestones and provide SMEs with the latest tools and insights to navigate cybersecurity compliance.

The website will also embed all OCCTET-related social media channels as well as direct links leading to the companies that make up the OCCTET Consortium.

As OCCTET's communication lead, DIGITAL SME will provide and manage key content to be published, while the ECLIPSE Foundation will coordinate and manage the main website's developments. The website can be reached at www.occtet.eu.

4.2.2 Social Media

To maximise the project visibility and reach out to all its target group with their preferred communication channels, OCCTET will use different means of communication including

LinkedIn, GitHub, Substack, Matrix and YouTube. These social media channels will help to maximise the project visibility via regular communication about the project's activities and results and will serve as relays for the website' posts (e.g. News, events announcement). These dedicated accounts will be regularly updated with the new content to disseminate results to a wide and targeted audience.

4.2.2.1 Social Media Engagement Strategy

The Social Media Engagement Strategy for OCCTET is designed to highlight the project's objectives and outcomes, motivate stakeholders to actively participate in project activities, and promote wider sectoral collaboration. This strategy will utilise selected social media channels to enhance OCCTET's brand recognition, create a consistent flow of information through the dissemination of news, results, and events related to the project. All activities will be aligned with OCCTET's broader communication objectives and principles, which include strong support for open-source solutions and adherence to EU cybersecurity policies. Dedicated hashtags will be developed to unify content and facilitate the searchability across platforms.

Social media posts will cover a range of topics and content areas such as:

- Promoting the OCCTET value propositions: posts will clearly communicate how OCCTET simplifies CRA compliance for SMEs by offering a free, open-source toolkit that reduces complexity and costs.
- Broadcasting CRA-related Information: posts will provide tailored information on the implications of the Cyber Resilience Act for SMEs, including tips, guidelines, and regulatory updates.
- The Open Source Community: regular updates will be shared that highlight expert knowledge, case studies, and success stories in managing cybersecurity risks with open-source solutions.
- Events: announcement and invitations to participate in project activities such as webinars, workshops, and expert selection events will be a central component of the strategy.

In addition to these topics, the strategy will include active outreach to relevant communities on various platforms. For example, on LinkedIn, the project will seek to engage with specialised groups such as Open Source-related communities.

Project partners, based on their internal communication strategies, are expected to support the dissemination of OCCTET's content. Specifically, partners are committed to reinforcing OCCTET communications by interacting with posts and content on their own organisational pages, amplifying the project's reach. This collaborative effort ensures that OCCTET's updates and key messages are consistently promoted across multiple channels and among diverse audiences.

To ensure that the impact of these activities is measurable, the social media analytics will be continuously monitored using a dedicated visibility tracker. This tracker will capture key

metrics such as post impressions, engagement rates (likes, comments, shares), and follower growth across all platforms. This systematic approach to analytics will help refine the engagement strategy over time, ensuring that content is optimised for maximum reach and impact. By combining targeted content, strategic outreach to relevant communities, formalised partner support, and rigorous data analysis, the strategy aims to maximise OCCTET's visibility and drive substantial engagement among end-users and multipliers alike.

4.2.2.2 LinkedIn

LinkedIn is the leading global platform for professional networking among individuals and businesses. Therefore, the LinkedIn page will primarily serve to increase awareness regarding the project in the Open-Source community and for SMEs who seek assistance in being CRA-compliant. As there is no character limit for posts on the platform, it will allow OCCTET to share some of its webpage contents directly on LinkedIn to increase engagement. Such "long reads" by expert stakeholders are very well received and widely shared. OCCTET can build on its Open-Source industry partners within the consortium to contribute to such posts.

DSME is responsible for the management of the LinkedIn account, and will post new content on a regular basis, no less than once a week. All involved partners are commited to contribute by boosting visibility of the OCCTET posts and by suggesting relevant content or drafting some of the technical posts.

OCCTET's LinkedIn Page can be found here:

https://www.linkedin.com/company/open-cybersecurity-compliance-toolkit-occtet

4.2.2.3 YouTube

The OCCTET YouTube channel will serve as the repository for long-form video content. This channel will host a variety of content, including product tutorials, expert interviews, webinars, and case studies that demonstrate how the OCCTET toolkit supports CRA compliance. Videos will be produced in high quality, with clear descriptions and dedicated hashtags to enhance discoverability. Regular uploads will ensure continuous engagement. The channel will also serve as an archive for past webinars and workshops, allowing stakeholders to access the content on demand.

OCCTET's YouTube channel can be found here: https://www.youtube.com/@occtetproject

4.2.3 Newsletter and email Campaigns

Email campaigns and newsletter will be used as direct communication tools with the OCCTET stakeholders.

4.2.3.1 Email Campaigns

Email campaigns will be an important tool for directly communicating project milestones and important updates to targeted stakeholder segments. Unlike press releases, which are

primarily aimed at the media, email campaigns are personalised communications that reach out directly to the OCCTET mailing list as well as to the networks of consortium partners. Key milestones for these campaigns include the project kick-off, major tool updates, and invitations to upcoming events such as webinars and in-person gatherings. Each campaign will feature clear calls to action, detailed project updates, and tailored content that addresses the specific needs of the recipients.

4.2.3.2 Press Releases

Press releases will be used to announce major milestones and strategic developments within the OCCTET project. The initial press release will introduce the project, outline its objectives, describe the consortium, and provide an overview of how the toolkit supports CRA compliance. Following press releases will focus on significant achievements, such as the release of the toolkit, key partnership announcements or key events organised in the project's framework. These releases will be distributed through traditional media channels, partners' own social media channels, and the official project website to maximise visibility and credibility in the broader market.

4.2.3.3 Newsletter

The OCCTET newsletter will be published on a regular schedule to provide an overview of the project's progress. It will aggregate key news, updates, success stories, and upcoming events. The newsletter will serve as an essential touchpoint for all stakeholders, summarising technical achievements, sharing case studies, and highlighting collaborative initiatives. It will also include links to detailed blog posts on the website, video content from the YouTube channel, and invitations to participate in webinars or workshops. This periodic communication will reinforce the project's value proposition and ensure that stakeholders remain informed about the project's development.

4.2.4 News Articles and News Updates

The OCCTET website will feature a dedicated news section where regular articles and updates will be published. These news items will provide in-depth coverage of project milestones, case studies, interviews with consortium partners, and the impact of the toolkit on CRA compliance. This section will not only support ongoing engagement but also serve as a valuable reference for the public and industry stakeholders interested in the project's outcomes.

4.2.5 Other Channels

OCCTET is also present on Bluesky, a decentralised social media platform that promotes open discussions and community engagement. Bluesky offers an opportunity to connect with developers, open source advocates and cybersecurity experts in a more decentralised and tech-focused environment, This platform will be used to share project updates, engage with

the open-source community and promote key discussions around CRA compliance. By leveraging Bluesky, OCCTET aims to reach a wider audience of innovators and developers, ensuring that its tools and resources gain visibility within relevant technical and policy-driven conversations.
OCCTET's Bluesky profile can be found here: https://bsky.app/profile/occtetproject.bsky.social

4.3 Events

4.3.1 OCCTET Events

In-person events constitute a key component of the OCCTET outreach strategy. These events, such as trade fairs, industry conferences, and roundtable discussions, are designed to showcase the project's outcomes, promote real-time engagement, and validate the toolkit through live demonstrations. In-person events will be planned with performance metrics tracked via KPIs such as the number of events attended or organised, the number of registered participants, and the level of engagement at each event. These activities will serve as both dissemination tools and as opportunities for gathering valuable feedback that will help refine the toolkit and further tailor the project's messaging.

4.3.2 Webinars & Workshops

Webinars and workshops are integral to OCCTET's strategy for educating stakeholders about CRA compliance and the practical use of open-source tools. An exemplary webinar has already been held in collaboration with the European DIGITAL SME Alliance, the European Cyber Security Organisation, and the Eclipse Foundation. Such events provide an overview of the CRA, outline its implications for SMEs and the open-source community, and offer expert guidance on adapting to new regulatory requirements. Interactive sessions will include live Q&A segments, panel discussions, and real-time demonstration of the toolkit once available. Key performance indicators for these events include the number of webinars or workshops held, participants counts, engagement rates during sessions, and feedback collected post-event.

4.3.3 Third-party Events

Throughout the project, OCCTET consortium partners will maximise the project's visibility by participating in third party events that are relevant to the project (e.g. FOSS conferences and fairs, industry events with focus on open-source solutions, etc.). This will be an opportunity to increase the knowledge around the project and engage closer with the OCCTET target audience. Thus, whenever possible, partners attending events will promote the project, e.g. by making presentations, bringing and sharing available dissemination materials, presenting posters, engaging stakeholders during face-to-face networking.

5 Operational Plan

5.1 Organisation and Implementation of the Activities

The organisation and implementation of the communication and dissemination activities are central to achieving OCCTET's mission of equipping SMEs with the tools and knowledge necessary to comply with the Cyber Resilience Act. This strategy integrates the project's technical deliverables with targeted outreach to ensure results are impactful, accessible and widely adopted. Monthly consortium meetings will include dedicated updates on dissemination progress, allowing for collaboration between technical and communication teams. These meetings will also serve as a forum to assess feedback from stakeholders, such as SMEs and FOSS developers, gathered during webinars and consultations. The results of these discussions will be used to refine messaging, content formats and outreach strategies. In preparation for major events or milestones, additional focused meetings will be held to coordinate partner contributions, ensuring cohesive and impactful campaigns.

Activities will be guided by a shared communication calendar, outlining key events, deliverables, and responsibilities. The calendar will allow all partners to align their efforts, avoid redundancies, and ensure the delivery of material. Throughout the projects DSME will implement a system of continuous monitoring and evaluation, ensuring the strategy adapts to stakeholder needs and maximises the project's visibility and impact.
In addition to awareness-raising activities, structured follow-up mechanisms are implemented to ensure continuity of engagement. These include post-event email communication to registered participants, onboarding to the OCCTET newsletter, invitation to join the project's wishlist for early toolkit access, and targeted outreach to SMEs expressing interest in pilot participation. This approach ensures that stakeholder engagement evolves from initial contact toward active participation in subsequent project phases.

5.2 Timeline of Dissemination and Communication Activities

The communication strategy for OCCTET follows a structured timeline aligned with key project milestones. Each phase employs specific communication channels and tools to engage stakeholders, ensuring progressive outreach that builds anticipation, drives adoption, and secures long-term impact.

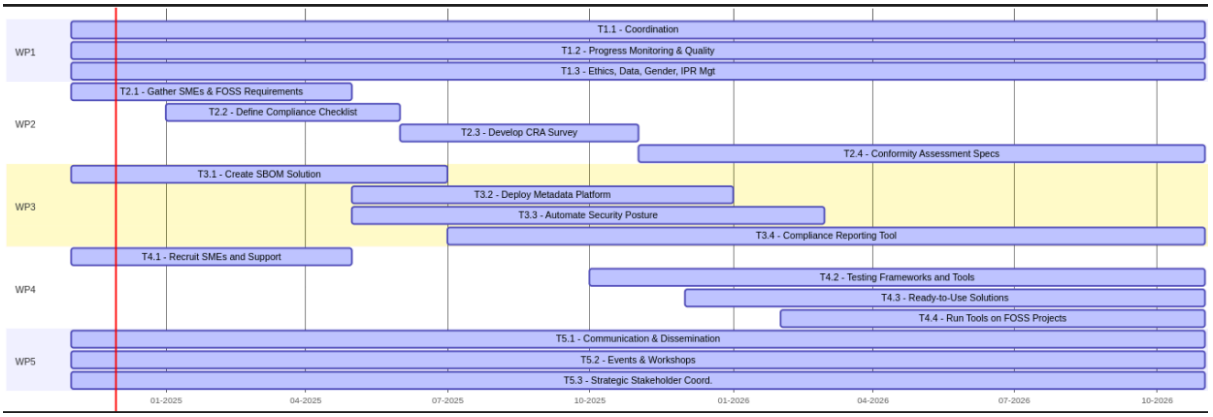
Phase 1 – Awareness and Preparation (M1 – M8): the project's initial phase focuses on establishing its identity and building a foundation for stakeholder engagement. During this phase, the OCCTET website and social media channels will be launched to serve as hubs for information and interaction. Branding materials, including the project's logo, templates,

and a tagline reflecting its mission, will be developed to create a consistent and professional image. During this phase, the OCCTET website and social media channels will be launched to serve as the central hubs for information and engagement. Branding materials including the project logo, templates, and key messaging, will ensure a professional and consistent identity across all communication channels. Stakeholders mapping will be conducted to identify and connect with SMEs, policymakers, FOSS developers, and cybersecurity experts, forming the foundation of OCCTET's outreach efforts. Face-to-face engagement will be prioritised through participation in industry events, cybersecurity conferences, and open-source forums, while targeted email campaigns will encourage stakeholders to subscribe for updates and follow OCCTET's social media channels. The first press release will formally introduce the project and its objectives, ensuring visibility within the cybersecurity and SME communities. Moreover, two needs analysis workshops will engage at least 25 SMEs each, allowing participants to share insights on CRA compliance challenges and contribute to shaping the toolkit's development.

Phase 2 – Dissemination of Key Deliverables (M9 – M20): This phase marks a shift toward actively promoting the OCCTET toolkit following its official launch. A press release will announce the toolkit's availability, emphasising its role in simplifying CRA compliance for SMEs. A series of interactive webinars and training sessions will provide practical guidance, including live demonstrations, case studies, and Q&A sessions to support early adopters. Social media engagement will intensify, featuring tutorial videos that will be available on the YouTube channel repository, and updates on toolkit developments. The use of dedicated hashtags will help expand engagement within relevant online communities. Regular newsletters and direct outreach campaigns will highlight user success stories and toolkit enhancements, reinforcing continued engagement. Blog posts and news updates on the website will provide in-depth analysis of CRA compliance, SME case studies, and expert insights on open-source security. OCCTET will also be showcased at cybersecurity events, SME-focused conferences, and government-led discussions to strengthen relationships with policymakers and industry leaders. By the end of this phase, OCCTET aims to have a growing community of SMEs actively using and benefitting from the toolkit.

Phase 3 – Sustainability and Impact (M20 – M24): This final phase focuses on ensuring the long-term adoption and continued relevance of OCCTET's result beyond the project's duration. Final webinars and training sessions will summarise the project's key achievements and provide stakeholders with a clear roadmap for ongoing use of the toolkit. The OCCTET website will transition into a long-term knowledge base, hosting compliance guides, training materials, and updated resources for SMEs and open-source developers. A final report, including best practices regarding the Toolkit, will be published and shared with industry bodies, reinforcing OCCTET's contribution to CRA compliance efforts. A concluding press release and summary materials will highlight the project's overall impact, securing its legacy within the cybersecurity ecosystem. Efforts will also focus on sustaining the toolkit's adoption through strengthened partnerships with Digital Innovation Hubs, FOSS communities, and cybersecurity networks, ensuring that OCCTET continues to serve SMEs and industry stakeholders as a reliable compliance resource.

The following GANTT chart outlines the key milestones and activities of OCCTET's communication strategy over the 24-month project timeline, divided into the aforementioned phases:



5.3 Partners' roles and responsibilities

The success of OCCTET's dissemination and communication strategy depends on the collaborative efforts of all consortium partners. Each partner brings unique expertise to the table, allowing a comprehensive approach to raising awareness, engaging stakeholders, and driving adoption of the project's results. The development and implementation of communication and dissemination activities are led by the European Digital SME Alliance.

As such, task leader DSME will be responsible for:

- Designing and executing the overall communication and dissemination strategy.
- Identifying key objectives, defining target audiences, and ensuring that activities align with the project's technical milestones and deliverables.
- Leveraging its extensive network in order to take the lead in reaching the primary audience for OCCTET.
- Content creation and management, including newsletters, press releases, case studies and video tutorial. This material is designed to translate complex technical outputs, such as CRA compliance.
- Managing the project website and social media channels including regular updates, engaging content and consistent branding.
- Gathering feedback from stakeholders, such as SMEs and FOSS developers during events and through digital platforms.

In addition, a significant contribution from all consortium partners is crucial for a successful implementation of this plan. Therefore, all partners are committed to contribute to the communication activities by carrying out the following actions:

- Contribution to content by providing technical input, reviewing drafts, and ensuring the accuracy of content related to their respective work packages.

- Participation in events such as webinars, workshops and industry conferences in order to enhance the project's visibility and credibility while facilitating direct engagement with stakeholders.
- Outreach through their networks to disseminate project outputs to regional and sector specific audiences, extending the reach of communication activities beyond DSME's core network.
- Social media engagement as a mean to amplify the project's messaging and ensuring it reaches diverse audiences

6 Impact and Performance Monitoring

6.1 Key Performance Indicators

By defining Key performance indicators (KPIs), the project partners will be able to measure and assess the effectiveness of the communication and dissemination strategy and to ensure that all the activities are being carried out according to the plan's objectives. For this purpose, the indicative KPIs that have been proposed in the DoA, and have been carefully elaborated by adding some new indicators and metrics, where necessary. These indicators will monitor progress across three distinct phases of the project implementation: pre-launch, post-launch, and post-project.

Pre-launch KPIs:

- Workshops: conduct two workshops with participation from at least 25 SMEs per session
- Events: attend at least three conferences or other in-person events, aiming to engage 100 SMEs who sign up for early access or express interest in the project
- Social Media Engagement: create project accounts on social media with a minimum of one LinkedIn post per week.
- Website features: launch a fully operational project website

Post-launch KPIs:

- Website traffic: achieve 10.000 visits by the end of the project with 1.000 total downloads or uses of the tools
- GitHub Engagement: facilitates at least 1.000 downloads/uses of the tools through GitHub
- Newsletter: publish at least monthly in the OCCTET Website
- Webinars: conduct three dissemination webinars, with 100 participants in total, focusing on tool usability and use case applications

Post-project KPIs:

- Tool Downloads: reach 300 downloads across 15 domains by M12, 600 downloads by M15 and 1.000 downloads in 30 domains by M18.

6.2 Monitoring and Reporting of the Indicators

Monitoring and reporting activities in the OCCTET project will focus on ensuring that the dissemination activities will be tracked using both event-based and digital channels.

Key monitoring methods include:

- Events-based monitoring: during the pre-launch phase, workshops and in-person events will be used as opportunities to gather feedback from SMEs and other stakeholders, ensuring the toolkit aligns with their needs.
- Workshops will track participation metrics, with a target of 25 SMEs per workshops, and ensure feedback is integrated into future developments.
- In-person events will measure engagement through attendee sign-ups, aiming for 100 companies to join the early access program or wishlist.
- Digital monitoring: the project's website will act as the central hub for monitoring visitor engagement, the use of interactive features and tool downloads.
- Social media platforms like LinkedIn will track engagement metrics such as post per week, reactions, shares, and comments.
- GitHub metrics will track tool usage and contributions during the post-launch phase with a target of maintaining active engagement among users and developers

6.2.1 Consortium Partner's Individual Communication and Dissemination Reporting

To ensure transparency, accountability, and alignment with the project's objectives, all partners are required to report their individual communication and dissemination efforts regularly. This reporting will focus on activities within the pre-launch, post-launch and post-project phases, contributing to the broader monitoring and performance evaluation framework.

Each partner will document their contributions to workshops and other in-person events, as well as monitor digital platforms including social media posts to promote the toolkit and engage target group and website contributions. Reports will also include any content developed by the partner, such as case studies, newsletters, or technical guidance, specifying the audience reached and the impact generated. Partners will also provide details of dissemination campaigns, including paid advertisements or targeted outreach efforts in specific regions or sectors.

Partners are required to submit detailed reports that will follow a standardised format provided by DSME to ensure consistency across all contributions.

All reporting will be centralised through the Visibility Tracker, and the data will be processed by the WP5 leader. The OCCTET Visibility Tracker is a structured tool designed to monitor, measure, and analyse the communication and dissemination activities of the project. It allows all consortium partners to log their contributions systematically and provides an overview of project reach and impact over time. The tracker consolidates data across multiple channels, including social media, events, press activities, and stakeholder engagement, to ensure that communication efforts are aligned with OCCTET's objectives and KPIs. The tracker consists of dedicated sheets for each partner, allowing them to individually log and monitor their communication effort. Moreover, a master sheet aggregates all data to provide a comprehensive view of the project's overall visibility.

6.3 Data Management

A detailed data management plan will oversee the collection, storage, and sharing of data throughout the OCCTET project, including key information from the toolkit and newsletter subscriptions. The data gathered from the toolkit will be carefully reviewed and shared to offer valuable insights into the project's progress and results, while ensuring privacy and confidentiality are maintained. Likewise, the data from newsletter subscriptions will be managed with the aim of keeping stakeholders and interested parties informed, all while fully complying with data protection regulations, such as the GDPR.

7 Annex A

Item Social Media Post/Event/ Newsletter/ Website article/ Press release	Social Media outlet	Link of the item	Number of Interactions	Publication date	Name of Event	Event Format	Role in event	Number of registrants	Number of participants
Social Media Post	LinkedIn	s/european-digital-sme-alliance_cyberresilienceact-	22	20/01/2025					
Event		https://www.digitalsme.eu/events/the-cyber-resilience-act-and-the-open-source-community/			The Cyber Resilience Act and the Open-Source Community: Understanding the Impact and Managing Comoliance	Online	Organiser	110	66

OCCTET PROJECT - Visibility Tracker

Total number of Social Media posts:	1
Total number of Social Media interactions:	22
Total number of organised events:	1
Total number of registrants to OCCTET events:	110
Total number of participants to OCCET events:	60
Total number of participations to external events:	0

Master Sheet | DSME | Eclipse Foundation | Double Open | Red Alert Labs | Bitsea | Expertware | AboutCode Europe

8 Annex B - Response to RP1 Review Comments

Comments	Actions taken
Minor documentation error	The duplicated sentence on page 5 has been removed. Formatting and structural consistency have been reviewed and aligned across the document.
Broaden and better target dissemination activities	The Target Audiences section has been clarified to explicitly distinguish between SME segments (FOSS developers, integrators, cybersecurity adopters) and ecosystem multipliers (EDIHs, NCCs). Tailored communication logic has been emphasised within the stakeholder engagement framework. A new introductory paragraph has been added before Table 3 in Section 6 - Target Audiences.
Strengthen quantitative evidence of reach and engagement	Baseline quantitative indicators from RP1 have been incorporated in the Technical Report, including stakeholder reach, SME registrations, event participation and structured workshop feedback metrics.
Elevate SMEs participation by targeting diverse segments and proactively include ecosystem stakeholders	The engagement of ecosystem multipliers has been further clarified in two sections: 1. Section 6 - Target Audiences (explicit inclusion of EDIHs and NCCs as multipliers) 2. Section 5.4, where targeted outreach to EDIHs and NCCs is now explicitly referenced as part of RP2 activities.
Improvements required in formatting to ensure consistency and compliance with reporting standards	A formatting review has been conducted across the document.

9 ACRONYMS AND ABBREVIATION

CRA — Cyber Resilience Act
ENISA — European Union Agency for Cybersecurity
EU — European Union
GDPR — General Data Protection Regulation
FOSS — Free and Open-Source Software
AI — Artificial Intelligence
IPR — Intellectual Property Rights
KPI — Key Performance Indicator
PII — Personally Identifiable Information
RBAC — Role-Based Access Control
SBOM — Software Bill of Materials
SAST — Static Application Security Testing
DAST — Dynamic Application Security Testing
MFA — Multi-Factor Authentication
SOC — Security Operations Centre
IR — Incident Response
API — Application Programming Interface
TLS — Transport Layer Security
ISO — International Organization for Standardization
IEC — International Electrotechnical Commission
ETSI — European Telecommunications Standards Institute
SUS — System Usability Scale
TRL — Technology Readiness Level
WP — Work Package
DoA — Description of Action

10 BIBLIOGRAPHY

1. **European Commission**, The Cyber Resilience Act — Questions & Answers, European Commission, 2024.
2. **European Commission**, DIGITAL Europe Programme – Model Grant Agreement, European Commission, 2024.
3. **OCCTET Project Consortium**, Description of Action (DoA), Grant Agreement No. 101190474, 2024.
4. **OCCTET Project Consortium**, CRA SME requirements and self-assessment checklists (D1.2), 2025.