



CYBERSTAND.eu

Engaging &amp; supporting EU experts in Cybersecurity Standardisation activities

Project Title	Engaging & supporting EU experts in cybersecurity standardisation activities
Project Acronym	CYBERSTAND.EU.eu
Grant Agreement No.	101158521
Start Date of Project	01.06.2024
Duration of Project	36 months
Project Website	<a href="https://Cyberstand.eu.eu.eu">https://Cyberstand.eu.eu.eu</a>

## D4.8 – SME engagement and consultation report – interim version |M18|

Work Package	WP2, [Pan-European standardisation efforts supporting implementation of the CRA]
Lead Author (Org)	James Philpot (DIGITAL SME)
Contributing Author(s) (Org)	Roberto Cascella (European Cybersecurity Organisation), Nick Ferguson (Trust-IT)
Due Date	30.11.2025
Date	28.11.2025
Version	1.0

### Dissemination level

( X ) PU: Public

( ) SEN: Confidential, only for members of the consortium (including the Commission)

## Versioning and contribution history

---

Version	Date	Author	Notes
0.1	21.10.2025	James Philpot (DIGITAL SME)	TOC and V0.1
0.2	21.11.2025	James Philpot (DIGITAL SME); Justina Bieliauskaite (DIGITAL SME)	First internal review
0.3	24.11.2025	James Philpot (DIGITAL SME)	
0.4	26.11.2025	James Philpot (DIGITAL SME); Justina Bieliauskaite (DIGITAL SME) Roberto Cascella (European Cybersecurity Organisation), Nick Ferguson (Trust-IT)	External reviews
1.0	28.11.2025	James Philpot (DIGITAL SME); Justina Bieliauskaite (DIGITAL SME) Roberto Cascella (European Cybersecurity Organisation), Nick Ferguson (Trust-IT)	Final version

### Disclaimer

This document contains information which is proprietary to the CYBERSTAND.EU.eu Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to a third party, in whole or parts, except with the prior consent of the CYBERSTAND.EU.eu Consortium.

# Table of contents

1	Introduction .....	10
2	SME Engagement Strategy .....	11
2.1	Rationale and Importance .....	11
2.2	Strategy .....	11
2.2.1	SME engagement .....	11
2.2.2	Phases of Engagement .....	12
3	SME Engagement report .....	15
3.1	Online engagement .....	15
3.2	Events .....	16
3.3	Other Actions.....	23
3.3.1	Mailings.....	23
3.3.2	Public Consultation .....	23
3.3.3	Cyber Resilience Act Support Community.....	24
4	Results and Impact .....	25
4.1	SSP Experts from SMEs .....	25
4.2	Results of Public Consultation.....	26
5	Next Steps .....	32
5.1	Future SSPs .....	32
5.2	Public Consultations.....	32
5.3	SME focused activities .....	33
5.3.1	Training and Educational Materials .....	33
5.3.2	Use Cases and Best Practices .....	33
6	Conclusion .....	35

## List of Figures

---

Figure 1 SME figures regarding applicants.....	25
Figure 2 "Have you heard of the CRA" responses .....	27
Figure 3 "In relation to digital products are you?" responses .....	27
Figure 4 Risk categorisation of products responses.....	28
Figure 5 Security requirements responses .....	28
Figure 6 Internal assessment responses.....	29
Figure 7 Documentation requirement responses.....	30
Figure 8 Reporting requirement responses .....	30

## List of Images

---

Image 1 Timeline of CRA implementation from <a href="https://Cyberstand.eu.eu/cyber-resilience-act-overview">https://Cyberstand.eu.eu/cyber-resilience-act-overview</a> .....	15
Image 2 Event banner 23.09.24 .....	16
Image 3 Event banner 26.02.25 .....	17
Image 4 Event banner 03.04.2025 .....	18
Image 6 Event banner 23.04.25 .....	19
Image 7 Event banner 08.05.25 .....	20
Image 8 Event banner 16.06.25 .....	21
Image 9 Event banner 19.06.2025 .....	22

## List of Tables

---

Table 1 How the outreach channels relate to each phase.....	14
---	----

# Terminology

Terminology/Acronym	Description
AE	Affiliated Entity
AI	Active involvement
AR	Awareness raising
CA	Consortium Agreement
CRA	Cyber Resilience Act
CRASC	Cyber Resilience Act Standardisation Community
CSA	Coordination and Support Action
DCESP	Dissemination, Communication, Engagement, and Sustainability Plan & Report
DEP	Digital Europe Programme
DoA	Description of Action
EC	European Commission
EDIHs	European Digital Innovation Hubs
EPE	External Pool of Evaluators
ESO	European Standardisation Organisation
EUOS	European Observatory for ICT Standardisation, available at <a href="http://www.standict.eu">www.standict.eu</a>
GA	Grant Agreement
KB	Knowledge building
KER	Key Exploitable Result
KPI	Key Performance Indicator
NSB	National Standard Body
OA	Open Access
PC	Project Coordinator
PMB	Project Management Board
PO	Project Officer
SB	Strategy Board

Terminology/Acronym	Description
SDO	Standards Development Organisation
SME	Small- and Medium-sized Enterprise
SSPs	Specific Service Procedures
TC	Technical Committee
TL	Task Leader
WG	Working Group
WP	Work Package
WPL	Work Package Leader



## Executive Summary

---

This document, D4.8 – SME engagement and consultation report – interim version, details the CYBERSTAND.eu project's strategy and initial outcomes regarding the involvement of Small and Medium-sized Enterprises (SMEs) in cybersecurity standardisation activities supporting the Cyber Resilience Act (CRA). SMEs are central to this project due to their vital role in the European digital economy and the widespread application of the CRA's mandatory requirements, despite their typical constraints in resources and budget for effective compliance with technical legislation. The project's engagement strategy is built on three key phases—Awareness raising, Knowledge building, and Active involvement—aimed at assisting companies with CRA compliance planning and integrating them into standardisation activities so that resulting harmonised standards are suitable for the SME context.

The interim results demonstrate success in actively involving experts from the SME community in standardisation efforts through financial support via Specific Support Procedures (SSPs). The successful targeting of these procedures was highly effective in attracting SME experts, whose contributions are expected to help reduce the regulatory and operational burden on SMEs by aligning CRA-oriented standards with practical frameworks and compliance tools. However, feedback gathered through the first public consultation highlighted critical knowledge gaps that require urgent attention. These results indicated that SMEs require more focused work on preparedness, particularly concerning the mandatory product security requirements of the CRA. Furthermore, a majority of SMEs reported difficulties in assessing their internal compliance capacity and struggled with implementing the detailed documentation and reporting requirements.

Based on these crucial findings, the second half of the project will pivot its focus to address the identified pain points in product security, documentation, and reporting. Future activities will include launching a second public consultation to validate the conclusions of the First White Paper (D2.2) and further investigate challenging requirements. The project will intensify its capacity-building efforts by developing and collecting targeted resources for SMEs. This resource production effort will concentrate on creating tailored SME guidelines for standards implementation, drafting or compiling comprehensive training courses and educational materials for an online repository, and identifying and showcasing use cases to demonstrate the beneficial application of standards for CRA compliance.

# 1 Introduction

D4.8 – SME engagement and consultation report – interim version, reports on the activities that the Cyberstand.eu project have undertaken throughout the first 18 months of the project period, from June 2024 to November 2025, to engage and activate small and medium enterprises.

SMEs constitute a key stakeholder group for CYBERSTAND.eu, primarily due to their significant role in the European digital economy (representing more than 99% of European companies). Given the CRA's mandatory requirements, which touch upon product design, component integration, and Open Source Software (OSS), the Act will apply to vast numbers of SMEs. However, these smaller companies typically possess fewer resources and a smaller budget compared to larger entities, making effective preparation and compliance with such technical legislation challenging. Therefore, providing resources—from requirements checklists to in-depth tools—is a vital function of the CYBERSTAND.eu project.

The project's SME engagement strategy is guided by two main, overarching objectives: firstly, to assist companies in **understanding the challenges for their compliance with the CRA**; and secondly, to integrate them into **standardisation activities**. Active involvement in standards drafting is crucial, as the final harmonised standards—which will offer a presumption of conformity under the New Legislative Framework—must be suitable and useable for SMEs to encourage greater adoption. The support offered by CYBERSTAND.eu, including financial assistance through Specific Support Procedures (SSPs) for experts, aims to make the CRA standardisation process supportive rather than burdensome for these companies.

The approach to engagement follows three broad, often overlapping, phases: **Awareness raising** (introducing the CRA and CYBERSTAND.eu funding opportunities), **Knowledge building** (helping companies deeply understand CRA provisions and creating a pipeline for experts), and **Active involvement** (facilitating participation in SSPs, promoting use cases, and gathering feedback through public consultations).

This interim report details the activities undertaken in the first half of the project. It outlines engagement actions such as the targeted use of online channels and dedicated events to promote SSP funding and CRA readiness. Furthermore, it reports on the successful engagement of SMEs in the SSP program and provides key findings from the first of two planned public consultations, which focused on SME preparedness for the CRA. The results of this consultation highlight critical areas where SMEs require urgent awareness raising and support, particularly concerning product security requirements, documentation, and reporting obligations under the CRA. Future activities outlined in this document include developing tailored SME guidelines, launching a second public consultation, and producing a comprehensive training and educational material repository.

This deliverable links closely with three other deliverables: D4.1, the Dissemination and Community Strategy, which identifies the project communication channels and SMEs as a key stakeholder and outlines how the project as a whole will undertake outreach to all stakeholders, including SMEs. In D4.2, the communication and dissemination results and activities are reported, which includes activities that are also reported in this deliverable. However, D4.8 focuses specifically on the relevance of these activities to SMEs, rather than the overall Cyberstand.eu audience.

D2.2, the first White Paper, will include the results of the public consultation and in turn will be validated through future public consultations, as well as identifying use cases that can be used to engage SMEs; and finally D3.2, the first Monitoring and Impact report which looks at the outcomes of the SSP experts work with the European SDOs and identifies how SMEs will be affected by the standardisation work, which is briefly discussed in this deliverable as well.

## 2 SME Engagement Strategy

The strategy set out below is intended to guide SME engagement and actions to support SMEs as they develop their understanding of the CRA and lead them towards contributing to the implementation and standardisation of the Cyber Resilience Act. Engagement was planned with two main objectives: to help companies with understanding and planning for their compliance with the CRA, and where possible, bringing them into standardisation activities so that the standards could reflect SME specific contexts and needs.

### 2.1 Rationale and Importance

SMEs (Small- and Medium-sized Enterprises) are a key stakeholder for CYBERSTAND.EU.eu for several reasons. Firstly, due to their role in the European digital economy (more than 99% of European companies are SMEs) the Cyber Resilience Act will apply to vast numbers of SMEs, and typically they are less able than larger companies to effectively prepare and comply with technical legislation. In particular, given the CRA's impact on product design and component integration, as well as OSS, SMEs will need to pay close attention to the CRA, given that they often relate to these roles and hardware manufacturers and software providers. However, SMEs often lack resources and budget to effectively manage their compliance; given that the CRA mandates that all products will have to comply with the requirements, SMEs can't simply declare themselves out of scope and continue business as usual. Therefore, providing resources for SMEs, from in-scope and requirements checklists to more in-depth tools, is a vital function of the Cyberstand.eu project.

Further to this, the Cyberstand.eu funding is a unique opportunity to bring more SMEs into the standardisation process. By involving more SMEs in the standards drafting process, it will ensure that the final standards are more suitable for the use of SMEs and therefore encourage greater use of the standards and therefore achieve compliance faster. For the CRA, given that the New Legislative Framework foresees that harmonised standards will give a presumption of conformity, it is crucial that the standards that are drafted to support the implementation of the CRA consider input from all stakeholders and company types, and are useable for SMEs. Therefore, the funding that Cyberstand.eu can offer to SMEs, as well as the support in onboarding to the SDOs and the different working groups is a crucial step to make sure the CRA standardisation process helps SMEs, rather than creates another set of tools that are too costly to implement.

### 2.2 Strategy

#### 2.2.1 SME engagement

The consortium includes the European DIGITAL SME Alliance (DIGITAL SME), the largest network of ICT SMEs in Europe, which is responsible for engaging the business community and ensuring their active involvement in standardisation activities and public consultations. The project also strengthened the participation of EU start-ups and SMEs in standardisation by establishing a dedicated facility to support EU experts contributing to standardisation efforts. Through Specific Support Procedures (SSPs), Cyberstand.eu provides financial assistance to European experts, especially targeting those from SMEs and start-ups.

Complementing the SSPs, the project dissemination and communication strategy (D4.1 section 3.3.2), also highlighted several specific activities to engage with SMEs with the project:

- **Trainings** – alongside the advisory material online, training will be offered through dedicated webinars and events to prepare companies for the CRA and explain standardisation. Discussed further in Section 5.3.
- **Public consultation** – multiple iterations of public consultation will be run to gauge SME readiness, pain points and needs to prepare for the CRA. Discussed in Sections 4.2 and 5.2.
- **Use Cases:** SMEs will be engaged to showcase how harmonised standards can be of applied in real world situations. Discussed in Section 5.3.
- **Cyber Resilience Act Support Community** – a group dedicated to knowledge exchange regarding standardisation and best practices regarding the CRA implementation. SMEs are encouraged to join the group to aid their preparations for the CRA. Discussed in Section 4.3 and 5.3
- **Events:** SMEs will be invited to participate in many of Cyberstand.eu's events, with several organised specifically for SMEs to seek their feedback and involvement. Discussed in Section 3.2.

Further to this, the online channels of the project such as the dedicated website (and partner websites), as well as social media, will be leveraged to share content targeted to SMEs and startups. The website and social are managed by Trust-IT as part of WP4 of Cyberstand.eu, and DIGITAL SME lead on SMEs and start up activities, providing content that was shared online specifically for SMEs and startups and organising events for the audience. The other project partners were all participants in events and were relevant created content or organised SME specific activities, such as the Community Groups in WP2 and in the particular the one on Standardisation (CRASC), lead by ECSO, or trainings on the SSPs, lead by Trust-IT and CEN-CENELEC, which while targeted to a broader standardisation audience were extremely valuable for engaging SMEs.

## 2.2.2 Phases of Engagement

To help with designing content and messaging to engage SMEs, three broad categories, or phases of engagement, were planned:

### 1) Awareness raising

This phase is the first introduction that the audience had to Cyberstand.eu, and to the CRA. This is a key stage for the SME audience, as many of them are not familiar with following cybersecurity legislation. Therefore, an engagement plan and accompanying materials were designed to enable SMEs to understand the relevance of the CRA, and what the funding opportunities offered by Cyberstand.eu represent. The messaging for these engagement actions reflected the timelines of the Act, who was likely to be affected and how they could engage with Cyberstand.eu to learn more, as well as the basics of standardisation. The SSPs (as a means of drawing attention), the CRASC and the online channels and events.

### 2) Knowledge building

Having first engaged SMEs through awareness raising, the next phase was built around helping companies to understand more deeply the provisions of the CRA, whether their product would be affected and the first steps they could take to begin preparing. Simultaneously, for companies that had relevant knowledge, this was the start of a pipeline to bring SME cybersecurity experts towards the SDOs and contribute to the standards drafting. The online channels and events are also important tools here for knowledge building.

### 3) Active involvement

The final phase is based around actively involving SMEs in the Cyberstand.eu activities. For standardisation, this means having successfully informed them of the standardisation process and funding opportunities that they are able to apply for SSP funding, and for CRA implementation where they are able to analyse their own readiness for the Act, and provide information on their gaps and needs, and even in some cases provide advice, regarding the requirements of the legislation. Activities to promote active involvement are the SSPs, use cases, trainings and public consultation.

These phases were not necessarily distinct and often overlapped, due to the complex nature of the CRA and the many topics and activities that it encompasses. Based on this, Cyberstand.eu's audience could require different messaging, perhaps even during the same event. For example, members of the Cyber Resilience Act Standardisation Community established under the Cyberstand.eu project as one of the Community Groups (see D2.2 for more details) might be very knowledgeable about the Act itself and the cybersecurity requirements, but not so knowledgeable about the standardisation request, so the messaging would need to include both awareness raising and promoting active involvement.

The table below highlights how the activities were used in the different phases, and how they can overlap.

Channel	Phase
SSPs	<p>Awareness raising (AR): funding support is a good hook to bring audience closer to Cyberstand.eu</p> <p>Knowledge building KB: SSPs are a topic that can be leveraged to educate SME audience about standards and drafting process</p> <p>Active involvement AI: encouraging SME participation in SSPs is a core activity of Cyberstand.eu</p>
Trainings	<p>AR: opportunity to participate in trainings is appealing to SMEs</p> <p>KB: trainings will develop SME preparedness for CRA, and improve their understanding of standards</p> <p>AI: through the CRASC, Cyberstand.eu will encourage SMEs to offer trainings or share resources/best practices with the community</p>
Public Consultation	<p>AR: the first public consultation is an opportunity to share baseline information about the CRA</p> <p>AI: responses from public consultation will be used to shape Cyberstand.eu output and activities</p>

Use Cases	<p>AR: Use cases will serve to highlight specific challenges that SMEs might face dealing with CRA compliance.</p> <p>KB: Use cases can give examples to other SMEs of how to prepare for CRA and use standards.</p> <p>AI: SMEs will be contributing their examples to Cyberstand.eu to be shared with the wider community.</p>
CRASC	<p>AR, KB: Cyberstand.eu will share a range of materials and organise activities that are intended to develop the knowledge and understanding of the CRASC on CRA, cybersecurity in general and standards.</p> <p>AI: members of the CRASC will be approached for involvement in other activities such as SSPs, trainings and events.</p>
Events	<p>AR: events will be one of the key tools that the Cyberstand.eu partners employ to share information regarding the SSPs.</p>
Online channels	<p>AR: the online channels for Cyberstand.eu will host and promote all relevant AR materials, such as recordings of events, informative pages and the public consultation, and will signpost where SMEs can go to either further develop their knowledge or become more actively involved (SSPs, use cases).</p>

*Table 1 How the outreach channels relate to each phase*

## 3 SME Engagement report

Several of the actions mentioned in Section 2.2.1 began in the first half of the project. Others, such as the training programme, development of guidance and guidelines and identification of use cases, will begin later once more content is available regarding the standards (such as draft texts) and more potential partners are identified (such as through the CRASC and DEP projects) to provide expert content. The activities that have been undertaken are explained in the following section, while the activities yet to begin are explained in Section 5.

### 3.1 Online engagement

A key channel through which SMEs have been engaged is via the websites of the respective partners and the main project website.

#### Cyberstand.eu website

While amplifying the main messaging of the project regarding the available funding, the Cyberstand.eu website began to collect and disseminate information to help companies learn about and prepare for the Act. **This began from a fundamental level**, first by highlighting the timeline of the implementation of the Act, to help companies recognise the urgency with which they needed to act. On this introductory page, alongside sharing an overview of the principles of the CRA, the timeline emphasises the deadlines for companies.

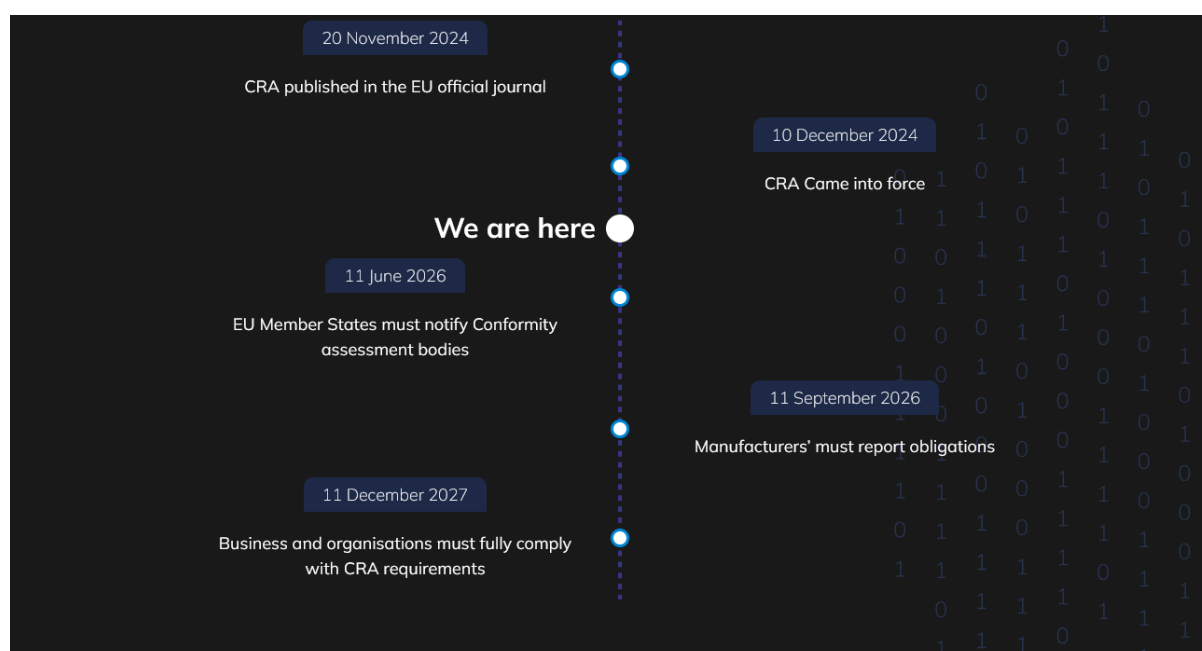


Image 1 Timeline of CRA implementation from <https://Cyberstand.eu.eu/cyber-resilience-act-overview>

Complementing this overview is a page dedicated to SMEs (<https://Cyberstand.eu.eu/smes-0>) which provides a more in-depth explanation of different aspects of the CRA. This page helps SMEs to judge at a glance whether the CRA relates to them and their products and services, and then offers a brief summary of the what the Act requires of them, and where they can go to obtain more information. The website also hosts the **public consultation** and **CRASC** overview and registration page.



Complementing the main project website, DIGITAL SME are also engaging SMEs to raise awareness about the CRA and the Cyberstand.eu funding support through their website. This is done highlighting the funding opportunities in the dedicated [funding portal](#), and offering CRA related advice and guidance through their [Cyber Resilience Hub](#) and [Information Sharing and Analysis Centre](#).

## 3.2 Events

This section presents an overview of the workshops, webinars and in-person events that Cyberstand.eu has organised. Not all these events were organised specifically for SMEs, but the focus or relevance for them has been highlighted.



*Image 2 Event banner 23.09.24*

**Supporting EU Experts in Standardisation Activities for the Cyber Resilience Act** (webinar, 23 September 2024). This webinar introduced SMEs and experts to the CRA standardisation request and how CYBERSTAND.EU offers support for those contributing via SSPs and working groups. It served as both an awareness-raising and recruitment tool. This event was supported by a targeted mailing that provided background, links to the event, and explained the value of SME participation in shaping CRA standards.

[Event link](#)

[Mailing link](#). Delivered to 2244 contacts of DIGITAL SME, with a 39% open rate and 104 clickthroughs to Cyberstand.eu's website.

**DIGITAL SME Summit: Breaking Europe's Digital Frontiers** (Conference, 10 December 2024)



Cyberstand.eu launched the first round of SSP funding at this event, hosting a booth at the conference and engaging companies and SME associations to promote the first round of funding to work on standards development. The event also discussed the Cyber Resilience Act and how it was likely to affect SMEs, and gathered stakeholders that would be able to provide support to companies to help them with their preparations for the CRA, who Cyberstand.eu were then able to engage.

[Event link](#)



*Image 3 Event banner 26.02.25*

**Standardisation for the Cyber Resilience Act** (webinar, 26 February 2025)  
This webinar focused on the CRA standardisation process, the support provided by CYBERSTAND.EU and how SMEs could apply for SSP funding. It was an entry point for SMEs to get involved in shaping applicable standards.

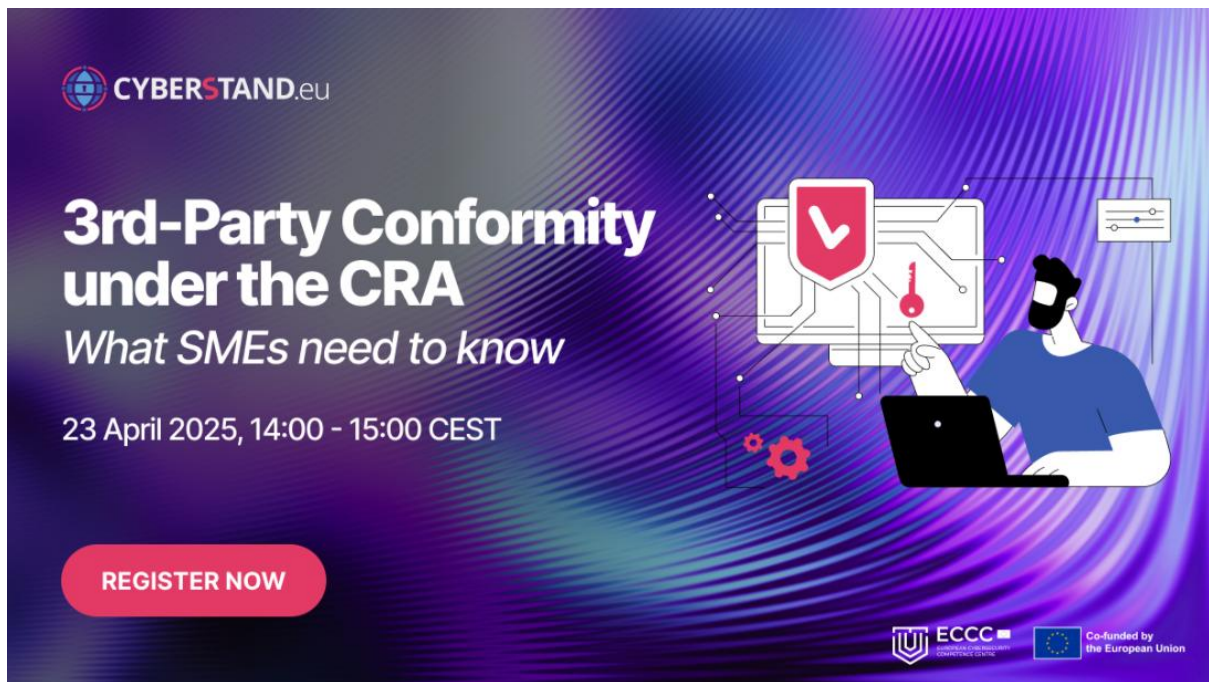
[Event link](#)



*Image 4 Event banner 03.04.2025*

**Standards and SMEs: How standards can benefit smaller enterprises** (Online workshop, 3 April 2025). This event looked at how small and medium-sized enterprises can turn standards from a challenge into an advantage. It highlighted how participating in standardisation can open doors to better business relationships, broader market access and technical innovation, rather than just being a cost or obstacle. The discussion also emphasised the need for more SME involvement in setting standards — because when standards are developed with SMEs in mind, they become more truly useful. The overarching message: by getting involved and taking advantage of standardisation processes, SMEs can strengthen their credibility, amplify their voice and create new opportunities.

Event link



*Image 5 Event banner 23.04.25*

### **3<sup>rd</sup> party conformity under the CRA** (online workshop, 23 April 2025)

The event “Third-Party Conformity under the CRA: What SMEs Need to Know” explained how the EU’s Cyber Resilience Act (CRA) will affect small and medium-sized enterprises, especially those manufacturing digital products. It clarified what third-party conformity assessments are, when they may be required, and how standards support compliance. The key message for SMEs was to prepare early—understand the assessment process, engage with relevant standards, and seek expert guidance to stay compliant and competitive under the new cybersecurity requirements.

[Event link](#)



Image 6 Event banner 08.05.25

### **How to write a winning SSP application: tips and guidance** (online workshop 8 May 2025)

This webinar helped experts interested in the SSPs to write better applications by offering guidance on the priorities of the CRA, the key deliverables from ETSI and CEN-CENELEC and the registration and application process. As a key target audience of the SSPs, who may not be familiar with applying for funding nor how the standardisation process works, the workshop gave help insight into what is expected of SSP experts and how they should structure their application.

Event link

Mailing link: 2543 deliveries; 35% open rate; 499 clickthrough



*Image 7 Event banner 16.06.25*

**From Regulation to Solution: How the Cyber Resilience Act is Reshaping the Cybersecurity Landscape** (online event, 16 June 2025)

This session highlighted how the CRA is changing cybersecurity expectations and introduced OCCTET's forthcoming toolkit for SMEs. Participants were invited to engage directly in the testing and development process.

Event link





*Image 8 Event banner 19.06.2025*

### **Impacting the CRA – Defining Standards for the Future** (Annual Event, 19 June 2025)

This flagship CYBERSTAND.EU event convened stakeholders from across Europe in Brussels to align on standardisation priorities for the CRA. SMEs participated in breakout sessions and live polls to voice needs, helping shape technical and policy recommendations. Promoted through a dedicated mailing campaign that encouraged broad SME attendance and input.

#### Event link

Mailing link (see public call for speakers below for audience details).

Alongside these public events, DIGITAL SME also regularly promoted Cyberstand.eu activities through its thematic Working Group events and to our wider community. Cyberstand.eu was presented at the Working Group cyber meetings on **12 November 2025**, which was a session dedicated to sharing the latest updates on the CRA with companies, and resources available to them to help prepare; on the **17 June 2025**, where the 7<sup>th</sup> SSP opportunity was promoted to the audience; and on 2<sup>nd</sup> June 2025 in the DIGITAL SME members meeting, as well as promoting the SSP opportunity in the WG Digitalisation meeting on 5<sup>th</sup> May 2025. Likewise, the first SSP was also promoted to members of DIGITAL SMEs WG Standards/SBS WG Digitalisation on 13 November 2024, a key audience comprised of standards experts from SMEs, and again on 24 April 2025.

Further to this, DIGITAL SME took part in the **DTX2025 event** in Cluj, Romania on 30 September 2025, where as part of a panel on “Trust by Design: Cybersecurity as a Foundation for Digital Society” they promoted the Cyberstand.eu funding and highlighted the project’s role in collecting and developing resources for SMEs to the industry audience in attendance.

## 3.3 Other Actions

### 3.3.1 Mailings

Several mailings were sent to promote Cyberstand.eu activities, outside of informing the audience about events or workshops:

- **Launch of Cyberstand CRA Working Group.** Sent October 23 2024 to 2288 recipients, promoting the launch of the CRAWG (now organised in three different Community Groups and one of them focused on standardisation CRASC). Had 883 unique opens and 253 clickthroughs.
- **Call for speakers: CRA roundtable at Cyberstand.eu event.** Sent May 27<sup>th</sup> 2025 to 312 recipients, to promote the Cyberstand.eu annual event and open a call for SME speakers to take part in a panel discussion on the challenges of the CRA for SMEs. Had 146 unique opens and 44 click-throughs.
- **Public Call for speakers: CRA roundtable at Cyberstand.eu event.** Sent to 703 recipients, this mailing promoted the Cyberstand.eu annual event and called for speakers to take part in the roundtable/audience discussion part of the aforementioned panel discussions, particularly seeking SME use cases regarding the CRA and standards. Had 280 unique opens and 141 clickthroughs.
- **DIGITAL SME Cyber Digest – September 2025** This regular newsletter included updates on CRA-related tools and events, such as the OCCTET community for early toolkit testing and a readiness survey for SMEs. It also highlighted guidance for CRA compliance and invited ongoing SME participation in shaping the ecosystem. Sent to 2304 recipients, with a 39% open rate.
- **DIGITAL SME Cyber Digest October 2025** This monthly newsletter shared similar messages to the September version, highlighting the funding opportunities available through Cyberstand.eu and tools and resources to help companies prepare for the CRA. Sent to 2352 recipients, with a 37% open rate.
- **DIGITAL SME Autumn 2024 Newsletter.** Sent in November 2024 to 4136 recipients, the newsletter promoted the launch of the 2<sup>nd</sup> SSP funding round to an SME audience,

DIGITAL SME created a [news article on their website](#) that shared the launch of the SSPs and background information on Cyberstand.eu, which has received 369 unique visits since being published.

The Cyberstand.eu project also released [regular newsletters](#), sent to a broad audience including SMEs, to promote specific aspects of the project, such as the launch of each funding round of the SSPs and the events that the partners organised or took part in.

### 3.3.2 Public Consultation

Cyberstand.eu planned two rounds of public consultation. The first was launched in summer 2025 and was focused on SMEs preparedness for the Cyber Resilience Act. The consultation can be found on the [Cyberstand.eu website](#), and also on DIGITAL SME's website. During the second half of the project, a second public consultation for SMEs will be launched.

The purpose of running public consultations is threefold. Firstly, it would support the implementation of the CRA by identifying pain points, blind spots and guidance needs for companies as they consider their compliance with the CRA. In particular, targeting the first public

consultation at SMEs allows for project activities to incorporate the needs of a key stakeholder group in ongoing activities from an early stage.

The second purpose of the public consultation is to raise awareness regarding Cyberstand.eu and the Cyber Resilience Act. Through basing the first consultation on the technical requirements of the Act, as well as exposing potential difficulties for companies, it can introduce the audience to the content of the Act in a simplified manner; therefore the consultation acts as both a market research tool and an educational tool. By allowing for different pathways through the consultation form, depending on their profile and product category, the users are able to learn how the CRA will relate to them and their product.

Finally, the public consultations will also be used to validate the White Papers that the project produces under task 2.1. Once these have been published, the research and conclusions will be incorporate into the following consultations and validated. The White paper has been presented in D2.2, with the support of the CRA Community Group and will be published in M18 of the project.

### 3.3.3 Cyber Resilience Act Support Community

Alongside the outreach and involvement in the SSPs, Cyberstand.eu intended to gather SME and cybersecurity experts into a Support Community. This was initially called the Cyber Resilience Act Working Group (CRAWG) but then was organised in three different Community Groups, including the [Cyber Resilience Act Standardisation Community](#). The initial Community Group was launched and coordinated by ECSO and detailed in D2.1. This group was intended to be a support group for the wider community, not just those experts selected through the SSP procedure. Interested parties could join the group to discuss the implementation process, identify challenges, share resources and discuss standardisation efforts with a peer audience, without being engaged through the SDOs or other formal mechanism. This would allow for discussions and exchanges between SMEs, OS operators, larger industry and standardisation communities, with Cyberstand.eu facilitating the meetings on a range of topics related to CRA implementation. The group would also act as a sounding board for conclusions drawn from the public consultations and White Papers.



## 4 Results and Impact

This section will discuss the results of the above activities, where applicable.

### 4.1 SSP Experts from SMEs

As mentioned previously, the SSPs were a key means of engaging SMEs with the Cyberstand.eu project, as the funding available was an important hook to engage smaller companies, alongside the support the project offered to companies that were knowledgeable cybersecurity, but not necessarily standards. This was a key tool for engagement across all three phases of outreach and was promoted through online channels and in-person and online events, as well as frequent mailings and personal outreach by all partners. As one of SSP's (SSP3) was specifically dedicated to attracting SMEs, this was given extra focus, through being launched at the DIGITAL SME Summit in December 2024, with an extremely relevant in-person audience gathered.

The outreach to SME experts to target their involvement in the standardisation drafting process can be considered a success. Across the 8 SSPs that were concluded at the time of this deliverable, 74 out of the 177 applicants to the SSPs were from SMEs (Figure 1). Out of this, 36 were successful, meaning that more than half of the funded experts were from SMEs. Further to this, the success rate of SME applicants compared to the overall success rate (48% compared to 37%) suggest that the efforts that the project undertook to target SMEs, and support their applications through advice sessions, was effective.

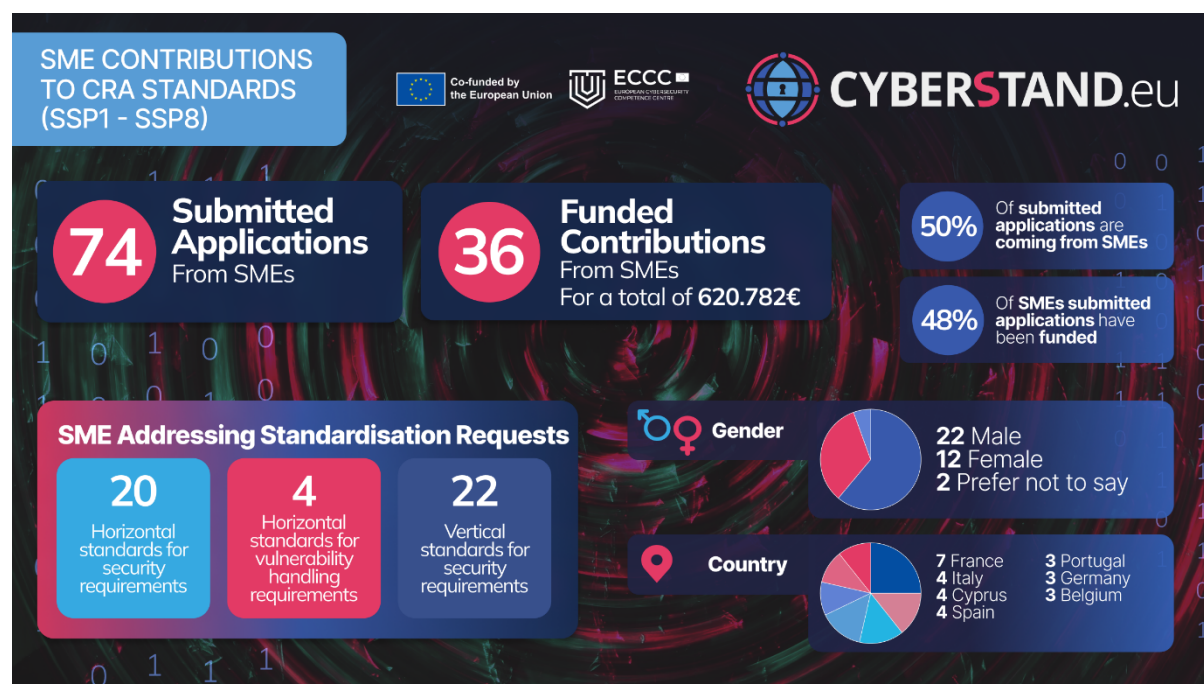


Figure 1 SME figures regarding applicants

Given that 52% of applications were not successful, Cyberstand.eu initiated a support process to help applicants to improve their applications, based on the feedback from the evaluators and colleagues from the SDOs. This took place through organising several follow up calls with applicants, to explain the criteria better, or identify a more suitable avenue for their work. In some cases, applicants were recommended for mentoring by SSP 01-52.

The results of this work and their contributions to the standardisation process are covered more fully in D3.2 Monitoring and impact report. Based on experience with other standardisation funding mechanisms, such as StandICT, and the general appearance of the working groups within the SDOs, it appears that Cyberstand.eu has been able to attract and onboard significantly more SMEs than is usual for this type of work, compared to the profiles of stakeholders funded through other mechanisms. Without insight into the full composition of the SDO Working Groups (which is not possible to obtain), this cannot be fully quantified.

The profile of companies selected are primarily European cybersecurity organisations that span consulting firms, product-security evaluation labs, cryptography specialists, cloud-security providers, and emerging-technology security innovators. As small to mid-sized firms, they are more focused on highly specialized domains, including hardware and embedded-device security, digital identity and trust frameworks, blockchain and quantum-resistant technologies, IoT compliance, and vulnerability research. Together, they form a diverse but technically advanced segment of the security ecosystem, who are highly relevant to the Cyber Resilience Act and would benefit from robust vertical standards to aid their compliance.

Based on the responses in the evaluation reports, the work of SSP experts will be beneficial for SMEs. The results show that respondents believe the work will help to reduce the regulatory and operational burden on SMEs by aligning CRA-oriented standards with familiar frameworks, open-source practices, and existing RED DA knowledge. Their contributions emphasise modular, risk-based requirements, practical templates, and automated compliance tools that SMEs can adopt without specialised legal or cybersecurity expertise. By promoting smart contracts, open-source ecosystems, and continuity with existing standards and frameworks, the work aims to make compliance more transparent, auditable, and cost-efficient. Overall, the responses indicate that the standards development process is expected to ease SMEs' transition to the CRA, lower implementation costs, enhance security posture, and support a more inclusive, scalable European cybersecurity environment.

The results and impact of the SSP experts is explained more fully in D3.2 Impact Monitoring Report.

## 4.2 Results of Public Consultation

The first public consultation received 168 responses, at the time of submission of this deliverable. Of the responses, 58 were from SMEs and they are reported and discussed in this deliverable. (The full results of the consultation are available in D2.2).

The first question of the Consultation was a framing device, to establish whether or not the participant was aware and informed of the details of the Cyber Resilience Act. If the response was "No", then the participant was directed to a page that explained the basics of the CRA, with links for further information.

As the results show (Figure 2), the vast majority of participants in the consultation were aware of the Cyber Resilience Act before participating in the consultation, which is likely a case of selection bias due to the consultation being hosted on the Cyberstand.eu and DIGITAL SME websites, which are most likely visited by more digitally aware companies. The consultation remained open for several months: from April 2025 to November 2025. When monitoring responses, we can see that the answers of "No" are predominantly distributed in the earlier responses, which might suggest that efforts at awareness raising regarding the CRA over previous months are having an effect.

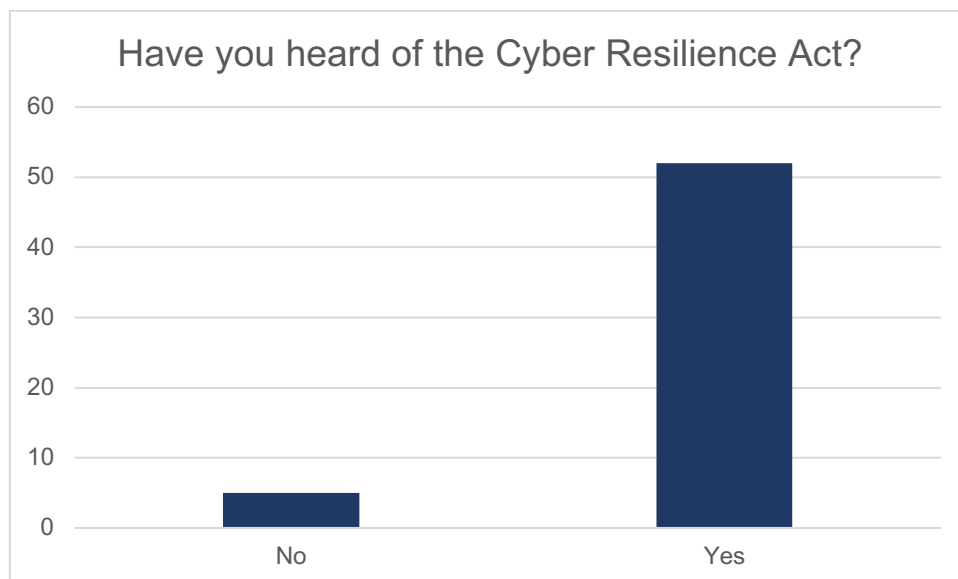


Figure 2 "Have you heard of the CRA" responses

SMEs that responded to the survey predominantly manufacture their own products (Figure 3); this suggests that they will need less advice regarding the compliance of third-party components within their products, which has been a concern raised in other fora.

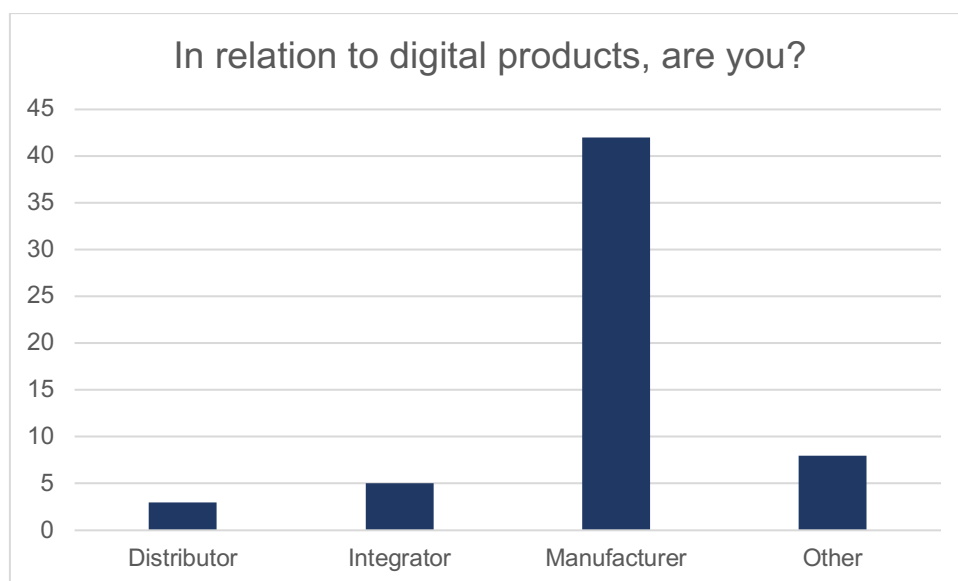
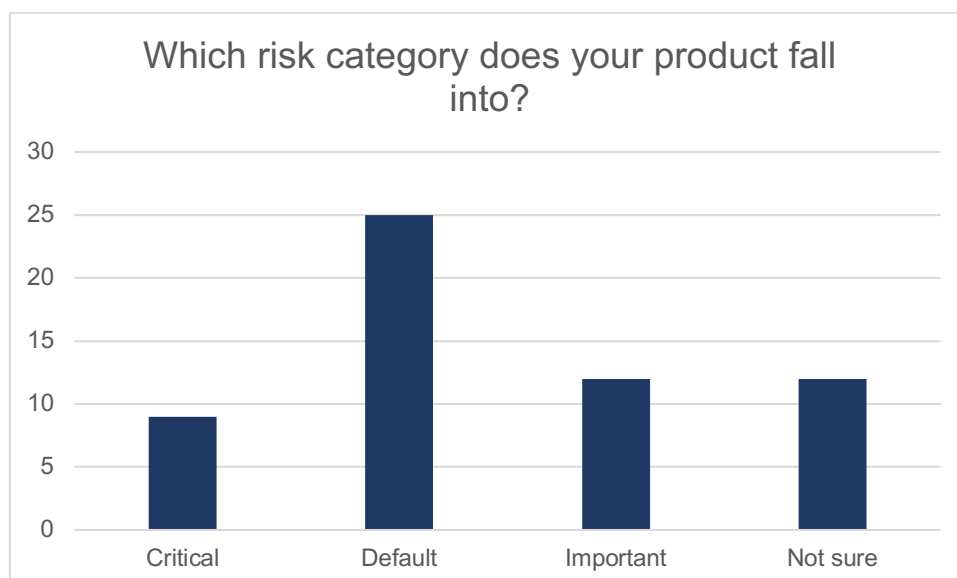
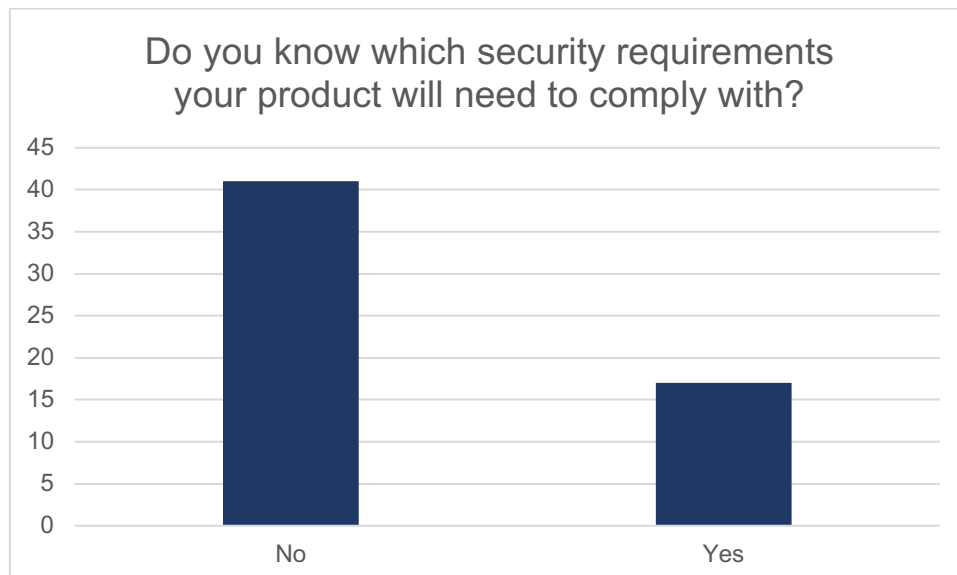


Figure 3 "In relation to digital products are you?" responses



*Figure 4 Risk categorisation of products responses*

Regarding the risk categorisation of products (figure 4), the overall response is positive as regardless of category, it appears that participants were able to identify which category their product falls under. When those that answered “Not Sure” were asked to share what their product was, the answers weren’t conclusive enough to be able to identify products that are currently outside the guidance lists provided in the annexes to the Act (“Software” was a common answer, as well as “router” which is already categorised).

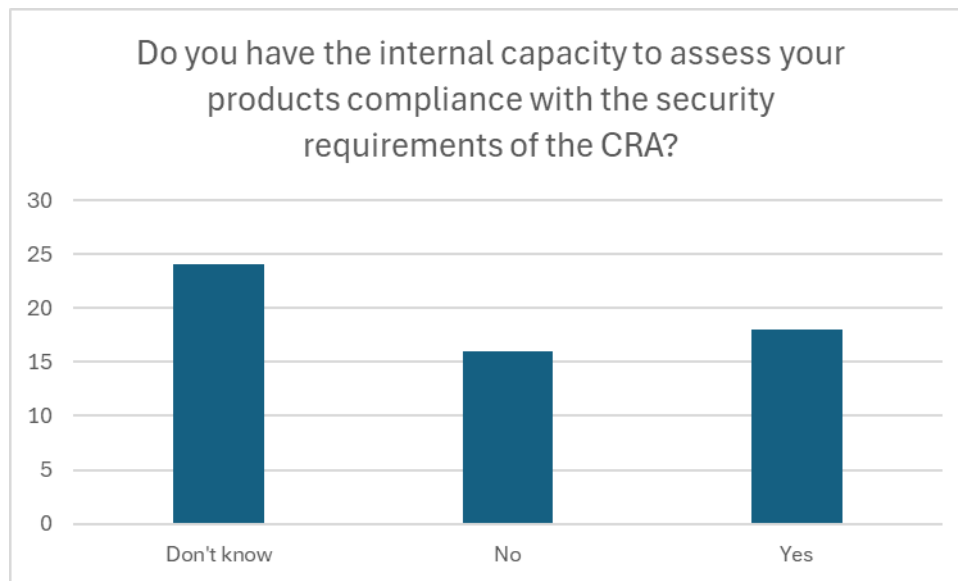


*Figure 5 Security requirements responses*

The latter questions in the consultation focused more closely on the detailed requirements in the Act. These questions are more targeted to those in the product development and maintenance process, given that they focus on the cybersecurity controls that need to be embedded in the product and the ongoing handling of cybersecurity through vulnerability management. The initial response, regarding the product security requirements (figure 5), indicates that clearly more work is required to raise awareness and prepare companies to ensure their product development is aligned with the CRA. Given lengthy product development timelines, ensuring companies are

aware of this will be a key focus on awareness raising efforts in the second half of the project. This consultation took the opportunity to share the security requirements with the participants that answered “No” and then followed up to ask whether companies could assess internally whether they were in compliance with the security requirements.

It appears that the companies that were already aware of the requirements are in compliance, whereas the majority are either unable to assess whether their security controls are in compliance, or are not sure (figure 6). This would suggest that more tools to aid with this are necessary, because products in the default category (the vast majority) would only need a self-declaration of conformity, yet the majority of companies would not currently be able to undertake this.



*Figure 6 Internal assessment responses*

There is more confidence in understanding the documentation requirements, with nearly half of SME participants in the consultation being capable of following the documentation requirements (figure 7). However, as more than 50% of participants weren't easily able to understand the documentation requirements, and therefore by implication, implement them, it suggests more work is required to provide guidance and tools on the documentation process.

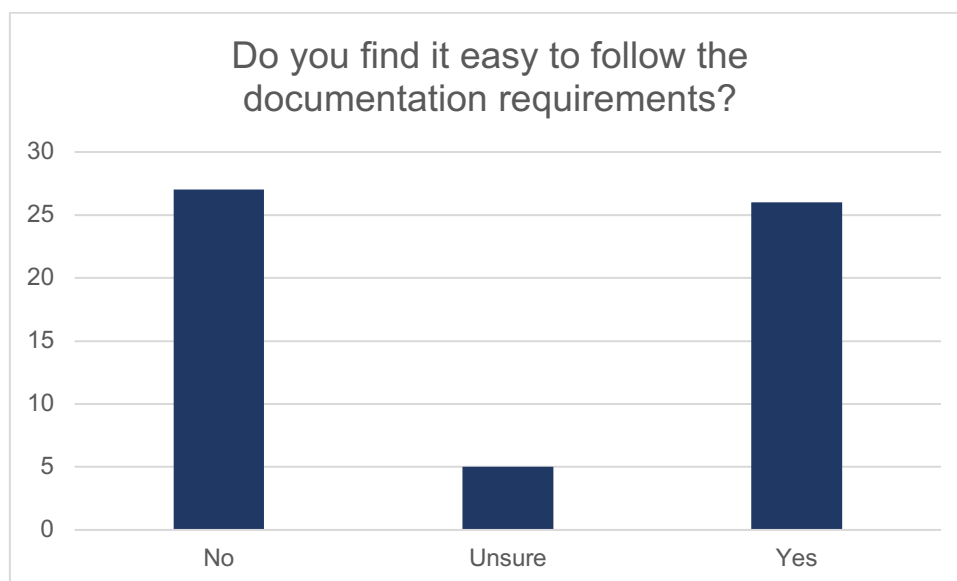


Figure 7 Documentation requirement responses

Regarding the reporting requirements (figure 8), the responses were broadly the same. Focus should be placed on guidance and supporting tools for reporting, and the follow up responses identified the 72-hour timeframe as a particular challenge. Developing tools that can automate or simplify the requirements help ease the reporting burden.

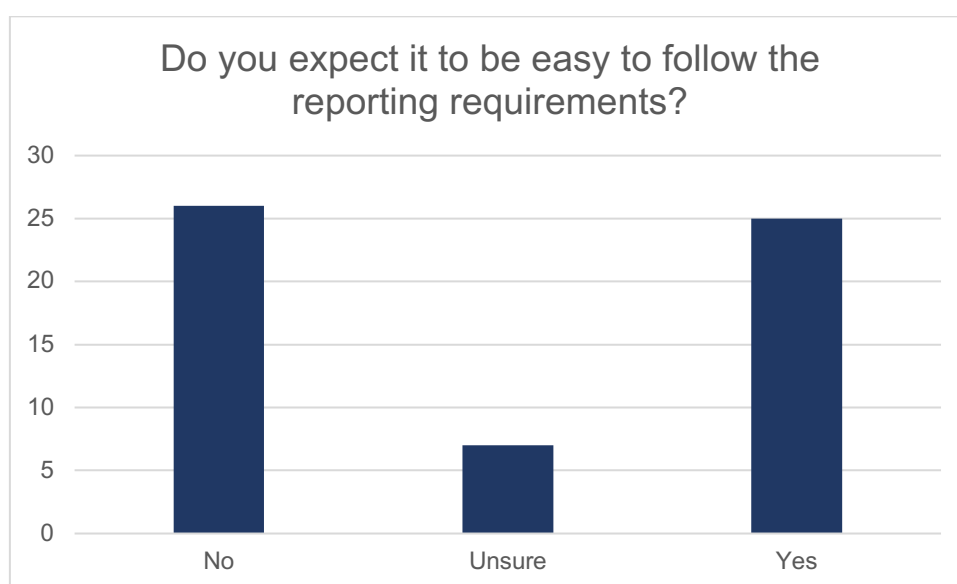


Figure 8 Reporting requirement responses

Based upon the results of the public consultation, it appears that Cyberstand.eu should mainly focus awareness raising and knowledge sharing on the product security requirements, as this was clearly highlighted as the largest area of concern for SMEs. Given the length of product development cycles and short amount of time remaining before the provisions of the Act enter into force, this should be treated with some urgency.

Cyberstand.eu is in a strong position to use the draft vertical standards to promote knowledge and understanding of the security requirements, as these can potentially be used as a form of guidance on how to develop a secure product, in line with the CRA requirements.

Further to this, more support should be developed to develop understanding of documentation of reporting requirements, and, where possible, identify tools and processes that can aid companies.

As reported in D2.2, if we compare the results gathered from SMEs with responses from all stakeholders (analysed in D2.2) there is much similarity. The main differences lie in the fact that SMEs have less clarity on understanding which risk category products fall into and are internally less clear on their internal capacity to assess product compliance.

## 5 Next Steps

### 5.1 Future SSPs

As of November 2024, the 9<sup>th</sup> and final SSP intended to fund experts to work on drafting the vertical standards closed. With the remaining funding, Cyberstand.eu could consider funding various activities to support SMEs preparations for the Cyber Resilience Act. These activities are under discussion and will be confirmed in the coming months.

- **SME Guidance for standards implementation:** Cyberstand.eu is considering funding either existing experts within the ESOs or others with a knowledge of and interest in SME needs to write guidance on how to implement the standards from the perspective of SMEs. It is important to note that this would be different to regular guidance on implementing standards, because many of the general assumptions about cybersecurity levels and controls within companies and product development do not apply to SMEs, particularly micro-SMEs, which are the majority of the market. Therefore, developing guidance which can advise on how the standards can be followed given the resources and capability restraints of SMEs, as well as the particular context (certain actions within the standards may not be relevant to SMEs, for example) of SMEs should aid the uptake of the standards, and promote compliance with the CRA. Discussions are underway to identify relevant members of the ESOs and pilot these activities.
- **SME Use Cases:** Cyberstand.eu will identify SME use cases, which will highlight beneficial applications of standards for SMEs. While generally, these will be funded, it might be in certain cases, such as piloting a draft standard to test its suitability, funding could be required to support companies to develop new use cases regarding the standards. This may be as simple as funding access to the CEN-CENELEC standards to develop the use cases.
- **SME readability/usability checks of draft:** alongside developing guidance and piloting the standards, it has also been suggested that SMEs could offer feedback on the draft standards in the form of “readability/suitability” checks, to help simplify the drafts and avoid using language and processes that SMEs, with assumed lesser technical capacity, may not be able to follow. To do so would require funding further experts to join the SDOs, or funding existing experts further.
- **SME Training Courses:** Cyberstand.eu will either draft or collect training materials to help SMEs understand and prepare for the different requirements of the Act. These may come from other EU-funded projects which are designing such material. Gathering these into one repository will avoid fragmentation of knowledge and help SMEs find official sources of information. This is further explained in Section 5.3

### 5.2 Public Consultations

A second round of public consultations will be launched in the second half of the project. The purpose will be to investigate further:

- **Outcomes from the first White paper:** this has been presented by ECSO in D2.2, and will look into issues and challenges of the implementation of the CRA, as well as possible solutions and resources. The 2<sup>nd</sup> round of public consultation will aim to identify further solutions, use cases and how serious the challenges of the CRA remain.



- Which requirements from the Act remain challenging: as mentioned, understanding where support is most required will become more important as the deadlines for compliance with the CRA approaches; therefore, Cyberstand.eu will aim to consult with companies, particular SMEs, to understand further what they still find challenging and where available resources are not sufficient. This will be particularly relevant to direct the actions of the CRA cluster, as the projects involved have significant capacity to identify and produce resources, and Cyberstand.eu will aim to effectively direct these efforts based upon feedback from the consultation.
- Types and forms of support required by SMEs to enhance adoption of standards: as the vertical standards become available, through efforts to pilot with different companies, Cyberstand.eu will aim to understand what challenges SME still face when using standards.

## 5.3 SME focused activities

The second half of the project will focus on producing resources for SMEs to enhance the uptake of the standards and increase preparedness for the CRA. When doing so, Cyberstand.eu will gather materials produced from external sources as well as develop its own resources, to try and offer a comprehensive library of resources to companies, and specifically SMEs. Through this collection, companies will be able to find support for specific aspects of the CRA or standards that they maybe struggling with, from official sources such as Member State National Authorities

### 5.3.1 Training and Educational Materials

CYBERSTAND.eu will create a comprehensive training programme for SMEs, based both on the Cyber Resilience Act and standardisation in general. The purpose will be to offer practical help for SMEs so that they are able to understand how they should approach the CRA, and how standards can help them: where to find them, how to implement them and whether they will need support to do so. These trainings will be delivered online by the project, while further educational material will be gathered and/or developed to be part of an online repository of supporting material.

This online repository will include advice and guidance developed by the CRASC, national authorities and the other CRA related projects funded by the DIGITAL European Programme. Cyberstand.eu will act as a multiplier and organiser of this community, to ensure that the produced materials are all available in the same location and are given prominence, while the efforts to produce such materials don't results in duplicated results.

The project will generate several policy- and standards-focused reports and guidance materials to facilitate CRA implementation and standard uptake. Specifically for SMEs, Cyberstand.eu will produce the aforementioned SME guidelines to the standards. Further to this, guidance will be produced to raise awareness on the CRA compliance requirements, explain the use of standards and where they can be obtained, and direct companies to where they can find further support. In essence, Cyberstand.eu will become a one-stop shop for support regarding both the CRA and the standards.

### 5.3.2 Use Cases and Best Practices

CYBERSTAND.eu will collect Use Cases relating to the demonstration of real-world scenarios related to the implementation of standards and preparations for achieving, and demonstrating,

compliance with the provision of the CRA by SMEs. This will ideally be achieved using the final versions of the standards, but if these are not available, it will be attempted with the draft versions.

The project aims to identify and showcase **30 use cases**. This will be facilitated via European Digital Innovation Hubs (EDIHs). The Use Cases will support the uptake of standards by highlighting to SMEs the benefits using standards in general, and when available, specifically the vertical standards to support compliance. Several use cases will be identified through the CRASC and documented in the first White Paper release. They will also be developed through the SSP experts and their contributions to the CRA standards drafts.

The results and feedback from these Use Cases will be shared with the European SDOs, especially the SME Working Group organised by CEN-CENELEC.

## 6 Conclusion

The interim period covered by this report, demonstrates significant progress in achieving CYBERSTAND.eu's core objectives of actively engaging Small and Medium-sized Enterprises (SMEs) in cybersecurity standardisation and preparing them for the Cyber Resilience Act (CRA).

A major success of the engagement strategy, which leveraged online channels, events, and mailings, was the outreach achieved through the Specific Support Procedures (SSPs). The project successfully attracted and funded 37 experts from SMEs across the concluded SSP rounds, meaning more than half of the total funded experts (65 in total) were from SMEs. Furthermore, the success rate for SME applicants (48%) exceeded the overall success rate (37%), suggesting that the targeted effort and supporting advice sessions provided by the project were highly effective. The work undertaken by these funded experts is expected to reduce the regulatory and operational burden on SMEs by aligning CRA-oriented standards with practical frameworks and compliance tools.

Despite these successes in expert engagement, the results of the first public consultation, which received 58 responses from SMEs, underscore significant challenges and knowledge gaps that require urgent attention. The consultation revealed that SMEs require more work to raise awareness and prepare for compliance, particularly regarding the specific product security requirements stipulated by the CRA. This area was highlighted as the largest concern for SMEs. Moreover, a majority of companies indicated they are currently unable to assess their internal capacity for compliance with security requirements, and over 50% reported difficulties understanding the documentation and reporting requirements. Notably, the 72-hour timeframe for reporting was identified as a particular challenge.

Based on these crucial findings, the second half of the CYBERSTAND.eu project will pivot its focus to address these identified pain points. Future steps will include launching a second public consultation to validate the outcomes of the First White Paper (D2.2) and to further investigate the remaining challenges SMEs face when adopting standards. The project will leverage the Cyber Resilience Act Support Community (CRASC), which successfully launched in October 2024, to gather feedback on tools and resources that can help address the identified difficulties in security requirements, documentation, and reporting.

The next phase will concentrate on producing and collecting resources for SMEs, which includes: developing tailored SME guidelines for standards implementation; drafting or gathering comprehensive training courses and educational materials for an online repository; and collecting and showcasing use cases to demonstrate the beneficial application of standards for SME compliance. These resources are vital to ensure that, as the deadlines for CRA compliance approach, SMEs have the necessary tools to navigate the Act effectively.