



**CYBERSTAND.eu**

Engaging & supporting EU experts in Cybersecurity Standardisation activities

# Supporting EU Experts in Standardisation Activities for the Cyber Resilience Act

**CYBERSTAND WEBINAR**  
23 September 2024

Post-Event report



Co-funded by  
the European Union



**ECCE**  
EUROPEAN CYBERSECURITY  
COMPETENCE CENTRE



Funded by  
the European Union

In today's rapidly evolving digital landscape, keeping up in cybersecurity is essential.

For professionals involved in EU cybersecurity, understanding the impact of the Cyber Resilience Act (CRA) and upcoming standardisation requests is crucial for shaping the security of digital products.

Under the CRA, any company aiming to enter the EU market must comply with strict cybersecurity standards.

This requirement raises the bar for safety and resilience across industries, ensuring that all products meet robust security criteria before reaching consumers.

This shift signifies the EU's commitment to a secure digital future, emphasising user protection and trust.

This webinar provided an in-depth look at the CRA's key components, outlined forthcoming standardisation requests, and presented a timeline for compliance. Engaging in these discussions helps professionals influence EU cybersecurity standards and contribute to a safer digital future.

The CYBERSTAND.eu project is a Coordination and Support Action focused on assisting Standards contributors, Open source contributors, SMEs and Product developers in developing and adjusting standards to meet the diverse requirements outlined in the Cyber Resilience Act's standardisation requests.

The event offered valuable insights into the CYBERSTAND.eu project, presenting its unique opportunities for cybersecurity experts, such as Specific Service Procedures (SSPs) that fund European experts' participation in cybersecurity standardisation, External Evaluators (EEs), and Cyber Resilience Act Working Groups (CRAWGs).

During the roundtable, experts shared practical perspectives on implementing the CRA and addressing its challenges.

Participants gained insights into the benefits of applying for SSPs, EEs, and CRAWGs, learning how their involvement can significantly impact the future of cybersecurity standards.

The CYBERSTAND.eu webinar attracted a diverse group of 178 registrants, with a strong representation from various European countries and even international participants from Japan and China.

Germany led in attendance at 17%, followed closely by Belgium (13%) and France (10%), reflecting the high interest in cybersecurity standardisation within these regions.

Gender distribution highlights a noteworthy level of diversity, with 66% male and 33% female attendees, a promising sign of increasing female representation in cybersecurity.

When it comes to webinar topics, interest in Specific Service Procedures (SSPs) was high, with 73 individuals expressing interest in applying.

This demonstrates a strong demand for financial support to foster comprehensive expertise in EU cybersecurity standardisation.

Additionally, 50 attendees were keen on joining the Cyber Resilience Act Working Groups (CRAWGs), highlighting the industry's proactive commitment to shaping cybersecurity standards.

Furthermore, 23 individuals showed interest in becoming External Evaluators, and 120 participants subscribed to the CYBERSTAND newsletter, indicating an ongoing commitment to stay informed and engaged with the project's activities.

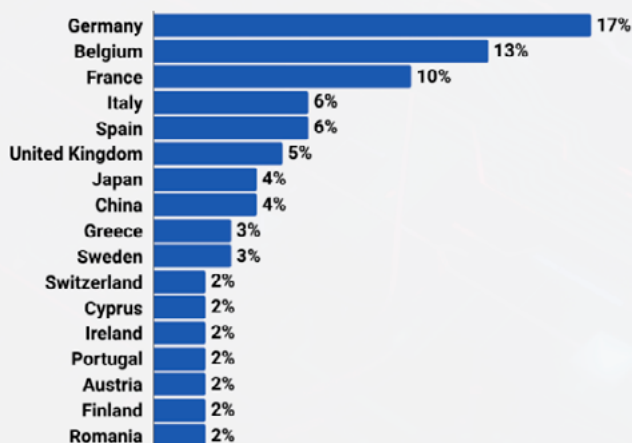
The variety in stakeholder representation adds depth to the discussion: 41.57% of attendees came from the industry sector, indicating that businesses are prioritising standard compliance to access and operate in the EU market.

Meanwhile, scientific organisations (15.06%) and cybersecurity entities (6.63%) underscore the blend of theoretical and applied perspectives in this evolving landscape.

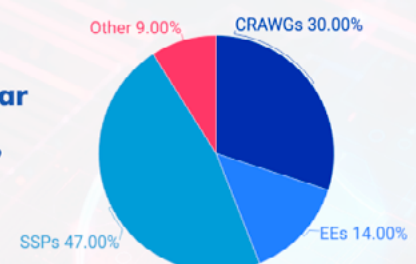

**CYBERSTAND.eu**
**Supporting EU Experts in Standardisation Activities for the Cyber Resilience Act**
**178 Registrants**
**Gender**

66%  33% 

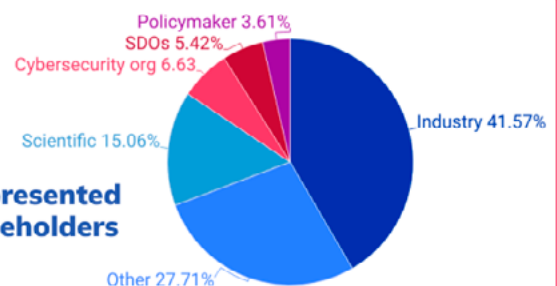
### % of participants by country



### Which webinar topic are you interested in?



### Represented stakeholders



# Event Takeaways:



Harmonised European standards will be critical to reduce the burden on manufacturers and facilitate CRA compliance by providing detailed guidance. The European Commission encourages manufacturers and other stakeholders to participate in standardisation work to shape these standards.



The timeline for CRA implementation is tight: the act is expected to be adopted in late 2024, with a 36-month transition period. The Harmonised Standards need to be developed within two years to ensure that they are available one year before the CRA becomes fully enforceable.



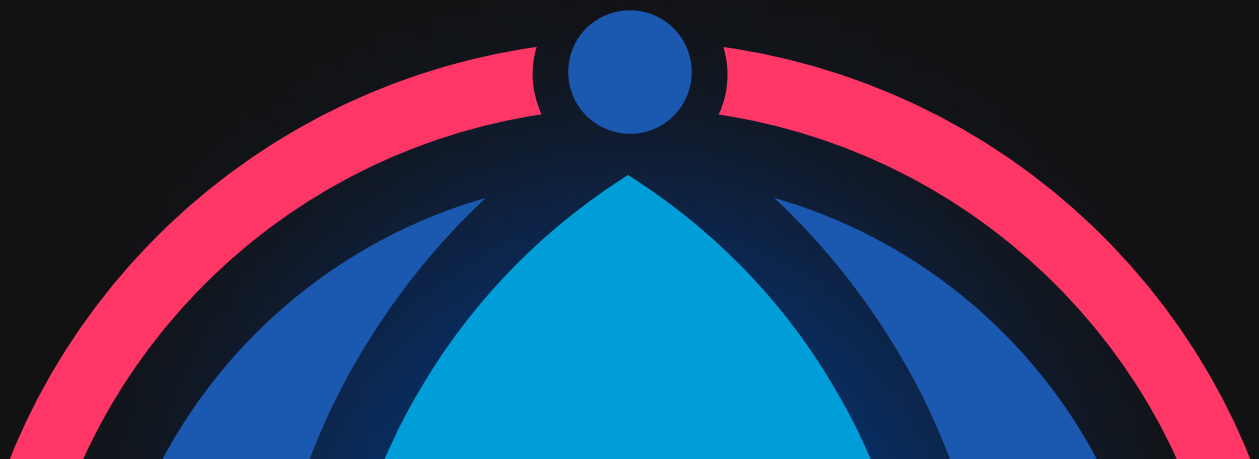
SMEs, startups, consumers, and the open-source community are often underrepresented in standardisation discussions, but their involvement is essential to ensure that the CRA standards are practical and inclusive.



The CRA addresses the entire product lifecycle, including design, development, and post-market phases, with obligations for vulnerability handling and reporting even after the support period ends.



The CRA's requirements are intended to raise the bar for cybersecurity across the board, but the path to full compliance involves complex, ongoing development of standards. The focus is on building a common language and coherent approach to cybersecurity that is applicable across different product categories.



## Insights from the experts:



*"Certain topics within the CRA are particularly relevant to consumers. Standardisation can be highly technical, making it challenging for consumer associations to participate effectively. Therefore, it is essential to consider consumer needs to facilitate their involvement in these discussions."*

**Filipe Jones Mourão** (Cybersecurity & Digital Privacy Policy, DG CONNECT, European Commission)



*"CYBERSTAND provides a platform for EU experts to contribute their knowledge and expertise to standards development supporting the CRA. This ensures inclusivity in the standardisation process by involving a diverse range of voices in developing cybersecurity standards."*

**Nooshin Amirifar** (CEN-CENELEC)



*"The CYBERSTAND CRAWGs are expert groups designed to facilitate discussions and foster dialogue between industry, SMEs, and start-ups regarding the CRA. Their goal is to drive collaboration and share insights on how to effectively comply with CRA requirements."*

**Matteo Molé** (ECSO)



*"SMEs are not yet fully prepared for the CRA. While the CRA's requirements are achievable for them, we have an opportunity to assess their current cybersecurity levels. This will allow us to tailor our efforts to raise awareness and provide targeted training, helping SMEs understand and comply with CRA standards effectively."*

**James Philpot** (DIGITAL SME)



*"A key goal of CYBERSTAND is to fund European experts' participation in cybersecurity standardisation through six cycles within the project's first year, each lasting 60 days. Only residents of the EU and associated countries are eligible to apply."*

**Teresa Ridolfi** (Trust-IT)



# CYBERSTAND.eu

Engaging & supporting EU experts in Cybersecurity Standardisation activities

## Watch the recording!

[cyberstand.eu](https://cyberstand.eu)



 [@CYBERSTANDEU](https://twitter.com/CYBERSTANDEU)

 [/company/cyberstandeu/](https://company.linkedin.com/company/cyberstandeu/)

 [zenodo.org/communities/cyberstand/](https://zenodo.org/communities/cyberstand/)

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



Co-funded by  
the European Union



ECCE  
EUROPEAN CYBERSECURITY  
COMPETENCE CENTRE