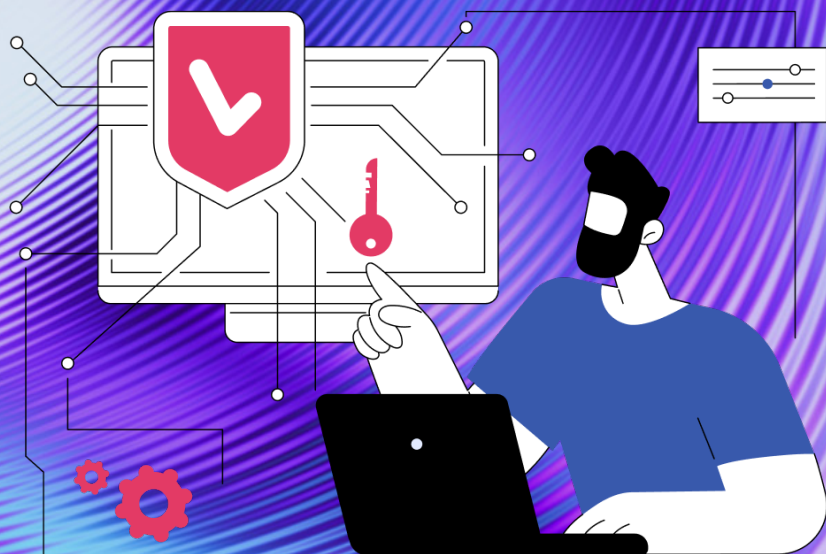




**CYBERSTAND.eu**

Engaging & supporting EU experts in Cybersecurity Standardisation activities

# Third-Party Conformity under the CRA: **What SMEs need to know**



**CYBERSTAND  
ONLINE WEBINAR**  
23<sup>th</sup> April 2025

Post-Event report



Co-funded by  
the European Union



**ECCE**  
EUROPEAN CYBERSECURITY  
COMPETENCE CENTRE



Funded by  
the European Union

Standards will be crucial to allow manufacturers knowing how to implement the essential cybersecurity requirements of the Cyber Resilience Act.

But they won't be useful only to manufacturers, they will also guide market surveillance authorities in enforcing the law, and support Notified Bodies in assessing product compliance.

While many manufacturers, particularly SMEs, may not have previously undergone a third-party conformity assessment, this may change depending on the product category your product will fall in, as well as the risk assessment you will perform as manufacturer.

This session is intended for market operators (especially SMEs), that would like to get started in understanding the process of 3rd party conformity.

This will be a high level introduction following this points:

- ▷ Introduction to TIC Council.
- ▷ Explain what a 3rd party conformity assessment is and its benefits.
- ▷ Why you might needed one in the context of the CRA.
- ▷ How are standards relevant for this?



## Event Takeaways:



The Cyber Resilience Act (CRA) will increase the need for third-party conformity assessments, especially for small manufacturers who may not have previously undergone such procedures. Depending on the product category or risk assessment, these assessments might become mandatory.



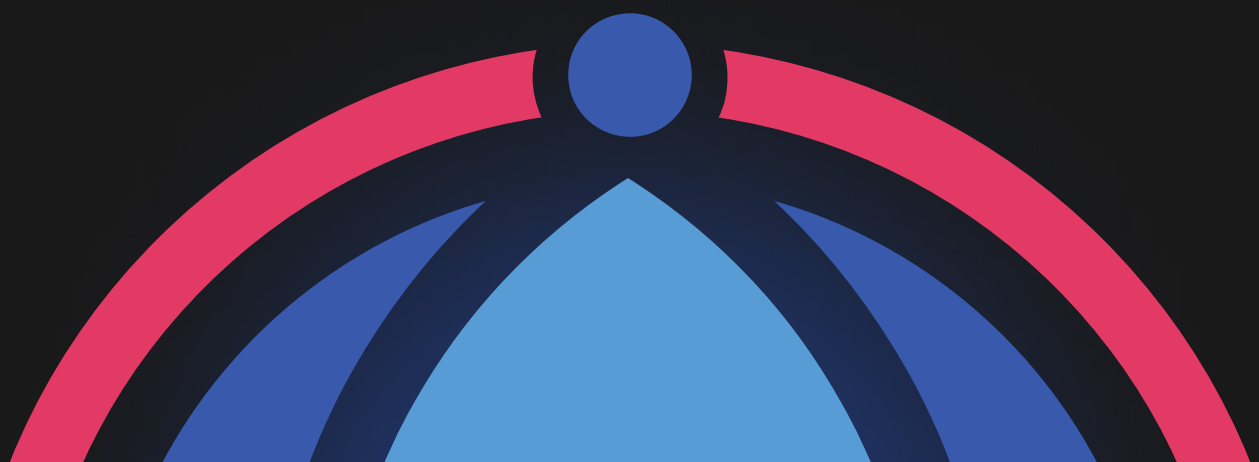
The TIC sector plays a dual role in cybersecurity by both supporting manufacturers in complying with EU legislation—through third-party conformity assessments—and offering voluntary certification schemes. Additionally, TIC companies invest in expert capabilities and collaborate with stakeholders to ensure effective enforcement and to shape future cybersecurity policies.



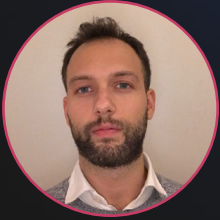
Under the CRA, the type of conformity assessment depends on both the product's risk level (e.g., critical or important products with digital elements) and the risk of non-compliance. Higher-risk products are required to undergo third-party evaluation, while lower-risk products may qualify for self-assessment.



Conformity assessments for cybersecurity products are complex, particularly when dealing with components that are certified through third-party assessments while others are self-assessed. There is an ongoing effort to develop guidance to facilitate the integration of self-assessed and third-party certified components.



## Insights from the experts:



*"Harmonized standards are not only useful for manufacturers, but they will be a reference also, they will be used by the bodies that perform third-party conformity assessments, but also by market authorities."*

**Matteo Molé**

(CYBERSTAND & Manager for Cybersecurity Technologies and Innovation, ECSO)



*"I think, at the end of the day, if in an organizations you're really actively engaged and care about the cyber security of your products, believe me, I think you're in a good position to be compliant with the CRA"*

**Ángel Moreno Rubio**

(Digital Policy Manager, TIC Council)





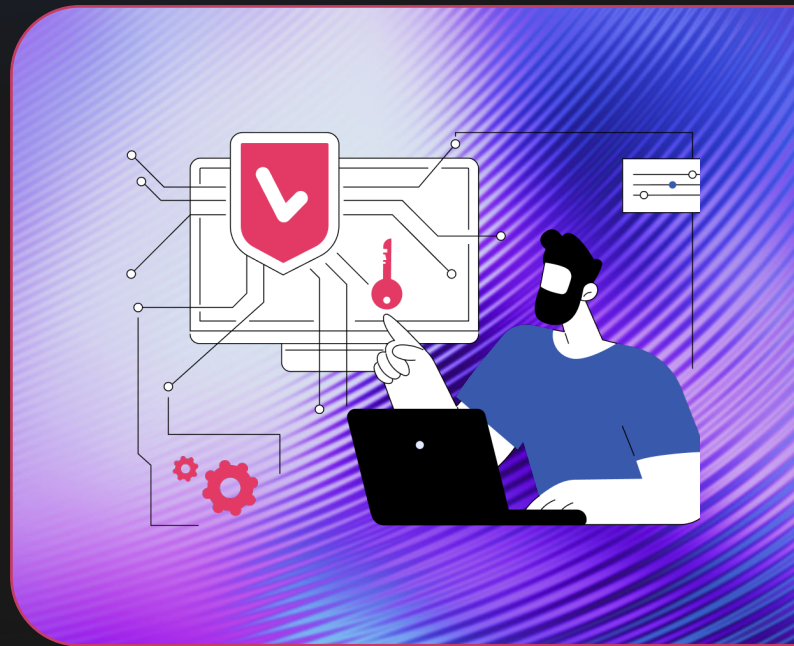


# CYBERSTAND.eu

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/cyberstandeu/)

 [zenodo.org/records/14046547](https://zenodo.org/records/14046547)

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



**ECCC**  
EUROPEAN CYBERSECURITY  
COMPETENCE CENTRE