



Independent Voice of Trust

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

Ángel Moreno Rubio, Digital Policy Manager

+32 2 880 21 37

secretariat@tic-council.org

www.tic-council.org

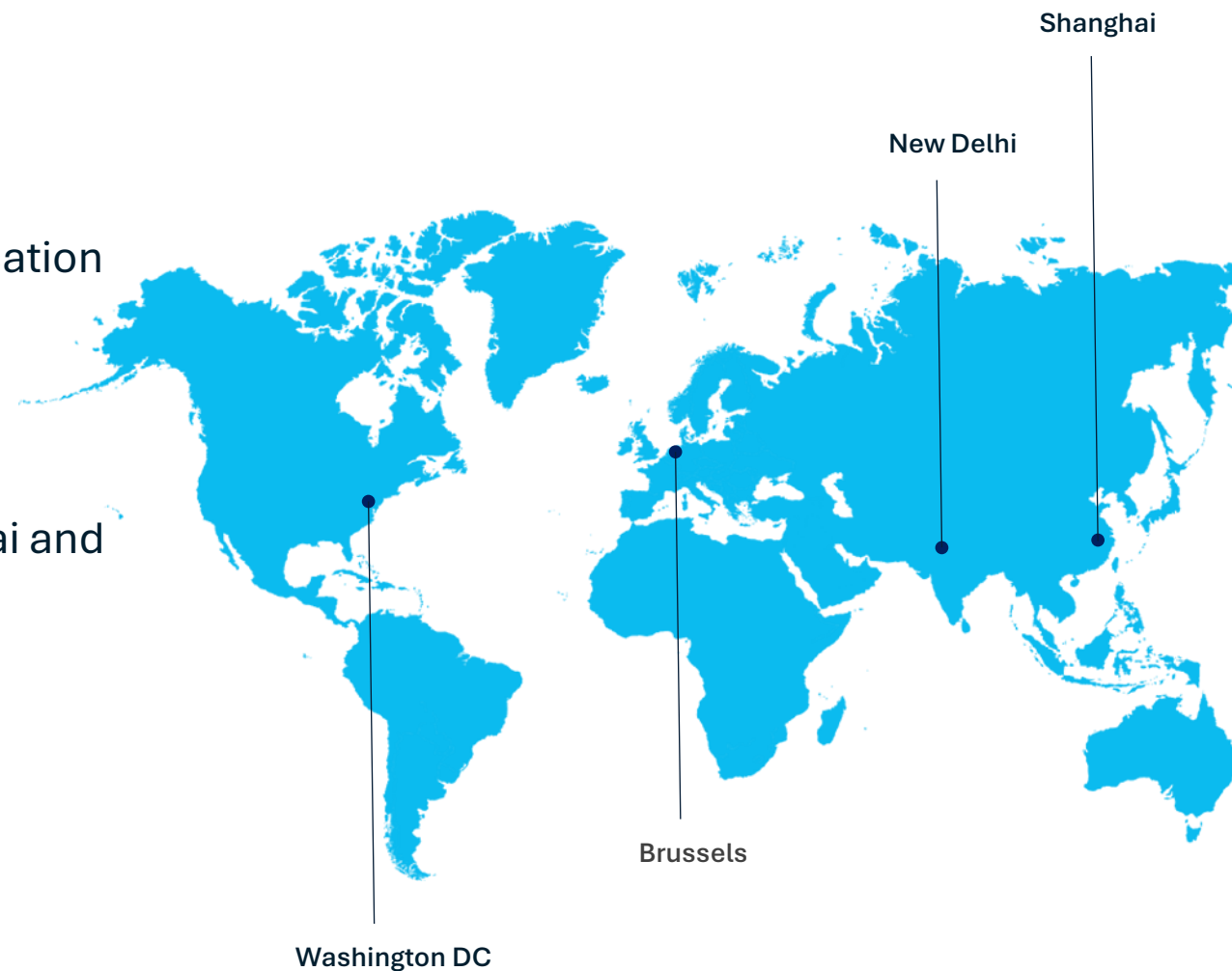
Agenda



- Introduction to TIC Council
- Explain what a 3rd party conformity assessment is and its benefits
- Why you might need one in the context of the Cyber Resilience Act (CRA)
- How are standards relevant for this?
- Q&A

About TIC Council

- The voice of the testing, inspection, and certification (TIC) sector.
- +100 Members active in +160 countries.
- Presence in Brussels, Washington DC, Shanghai and New Delhi.



TIC Council Strategic Objectives



ADVOCACY

Advocating for a balanced and informed regulatory framework



REPUTATION

Enhancing the reputation and raise awareness of the role of independent TIC



BEST PRACTICES

Raising standards of the TIC industry's practices in order to enhance trust in the TIC industry

TIC Council's Key Policy Areas



SUSTAINABILITY

Our members offer sustainability due diligence throughout manufacturing processes and supply chains. This may include conformity with environmental requirements, equality policies, human rights protection and healthy working conditions throughout the value chain.



PRODUCT SAFETY & COMPLIANCE

Our members conduct conformity assessments of products regarding electrical, mechanical, food, health and chemical safety as the general protection of consumers against unhealthy or dangerous products.



DIGITALISATION

Our members test digital solutions and products against connectivity, cybersecurity, privacy and safety requirements. This may include malicious code and penetration testing, interoperability testing or electromagnetic compatibility testing.



INTERNATIONAL TRADE

The TIC sector facilitates trade by enabling economic operators to test and certify their products with the requirements of other world regions. Thereby, economic operators can export their products and participate in high – level value chains.

TIC sector's role in cybersecurity



- Working across sectors to evaluate, mitigate and address cyber risks throughout the life cycle of products/services.
- Supporting manufacturers in complying with cyber legislation via third-party conformity assessment and issuing voluntary certification schemes.
- Investing in the knowledge and skills of our experts.
- Collaborating with stakeholders to:
 - ✓ Ensure the effective implementation and enforcement of existing EU cybersecurity legislation.
 - ✓ Provide TIC sector expertise and guidance in shaping future EU initiatives.

Working to improve cybersecurity?



You may not know the Testing, Inspection and Certification (TIC) sector yet, but...

► We are:

- ◉ Supporting manufacturers in complying with cybersecurity legislation across the world via third-party conformity assessment.
- ◉ Working with a range of different sectors from consumer electronics to medical devices to evaluate, mitigate and address cyber risks throughout the life cycle of a product or service.
- ◉ Continuously investing in the knowledge and skills of our expert staff to stay ahead of technological change and fast-moving cybersecurity challenges.



► We consider:

That the EU is the global leader in developing a regulatory framework for safe and secure connected devices. However, a wave of new legislation including the **Cyber Resilience Act** and the **Radio Equipment Directive Delegated Act** presents challenges for manufacturers. Many companies, in particular SMEs, do not necessarily have the internal know-how or resources to ensure compliance, particularly when technical guidance and implementing rules in these areas are still being developed. If left unaddressed, these challenges could jeopardise the safety, security and privacy of consumers, businesses and public administrations.

► We call for:



The inclusion of appropriate third-party conformity assessment requirements for high risk/critical products in all relevant EU legislation relating to cybersecurity.



The involvement of the TIC sector in the design of implementing legislation and guidelines for the Cyber Resilience Act.



Political support for faster and more efficient standardisation processes for consumer devices and critical infrastructure to provide certainty for all stakeholders involved in cybersecurity.

The Testing, Inspection and Certification (TIC) sector provides independent evaluation, validation, testing, quality inspection, system verification and certification services across practically all economic activities, including manufacturing, construction, energy, healthcare, food and beverages. With an array of cutting-edge laboratories and a highly skilled workforce, the TIC sector plays a critical role in ensuring consumers, infrastructures and businesses' safety and security through the engagement and on-site work of qualified experts, including engineers, inspectors, auditors, doctors and biologists.

Read our [white paper on connected devices](#).

The basics

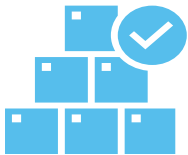


Conformity assessment – “*Process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled*” (Regulation (EC) 765/2008)

“*Process of verifying whether the essential cybersecurity requirements set out in Annex I have been fulfilled*” (Cyber Resilience Act)



Conformity Assessment Body (CAB) – “*Body that performs conformity assessment activities including calibration, testing, certification and inspection*” (Regulation (EC) 765/2008)



Notified Body (NB) – “*Conformity assessment body designated in accordance with Article 43 and other relevant Union harmonisation legislation*” (Cyber Resilience Act)

NBs are designated by Member States under specific legislation to perform conformity assessment tasks required for CE-marking certain product categories.

Useful
sources

New Legislative Framework (2008) + Blue Guide (2022)

Types of conformity assessments – 1st party




FIRST-PARTY

SECOND-PARTY

THIRD-PARTY

- ✓ **Who:** Performed **by the organisation** that provides the object.
- ✓ The manufacturer **demonstrates that a product/service fulfils specified requirements.**
- ✓ Used when there is a **lower level of risk** associated with non-compliance and with the product.

For a First-Party conformity assessment to work:

-  The risk of non-compliance must be low.
- 
-  The risk of the product must be low.

Types of conformity assessments – 2nd party

FIRST-PARTY

SECOND-PARTY

THIRD-PARTY

- ✓ **Who:** Performed by a “party having an interest in the object of conformity assessment” (e.g., buyer, user association, customer-contracted tester).
- ✓ Customer-commissioned testing or inspection performed by a supplier’s trading partner.
- ✓ More objective than first party; aligns with the purchaser’s risk profile.

Types of conformity assessments – 3rd party

FIRST-PARTY

SECOND-PARTY

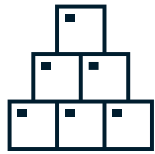
THIRD-PARTY

- ✓ **Who: Independent, external bodies** with no commercial stake in the outcome.
- ✓ **Accredited or formally designated bodies** perform testing, inspection, or certification.
- ✓ Highest impartiality and credibility; can be required by regulation (e.g. Cyber Resilience Act).

Third-party is widely relied upon in many markets when:

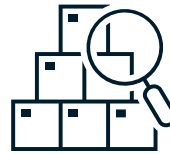
- There is a higher risk associated with non-compliance.
- There is a higher risk from products/services.

How does third-party conformity assessment work?



STEP 1

Labs receive samples from manufacturer and review documentation



STEP 2

Labs conduct testing **against standards**

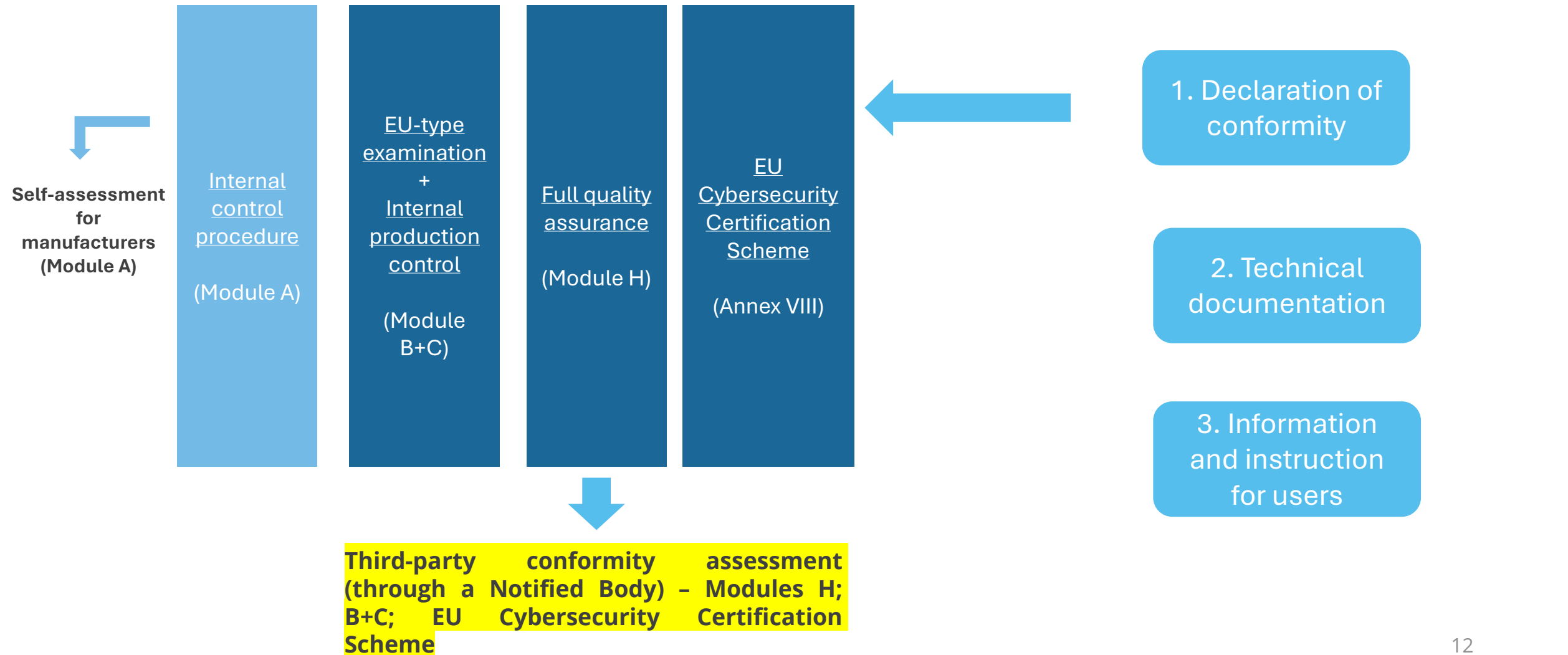


STEP 3

Labs produce test reports with pass/fail result

Conformity assessment under the CRA

Conformity assessment procedures (Art. 32 & Annex VIII)



CRA – product categorisation

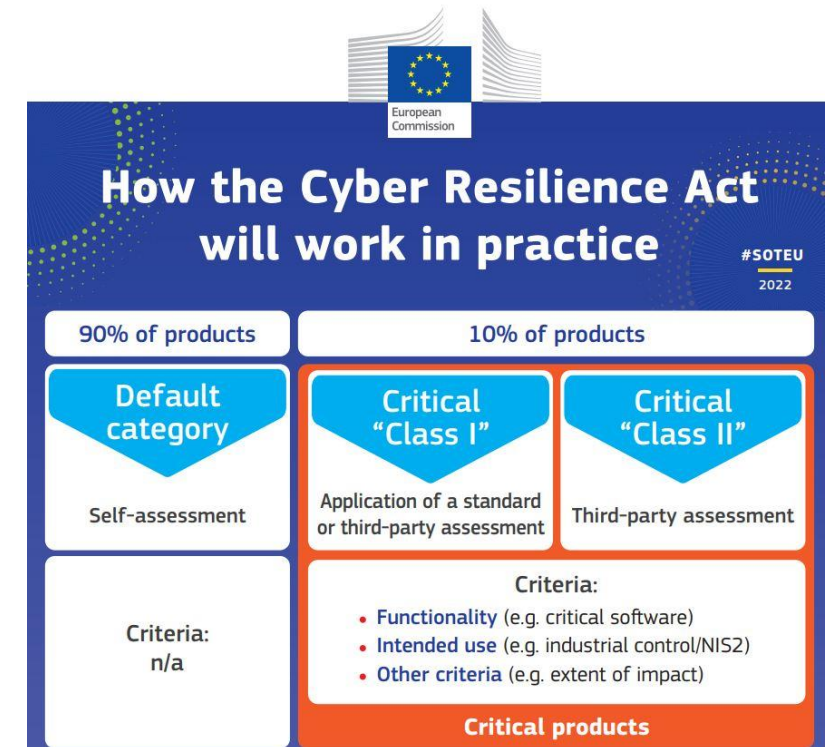
Important products with digital elements – Annex III

- Class I: Identity management systems, standalone and embedded browsers, operating systems, routers, etc.
- Class II: Firewalls, intrusion detection and prevention systems, etc.

Critical products with digital elements – Annex IV

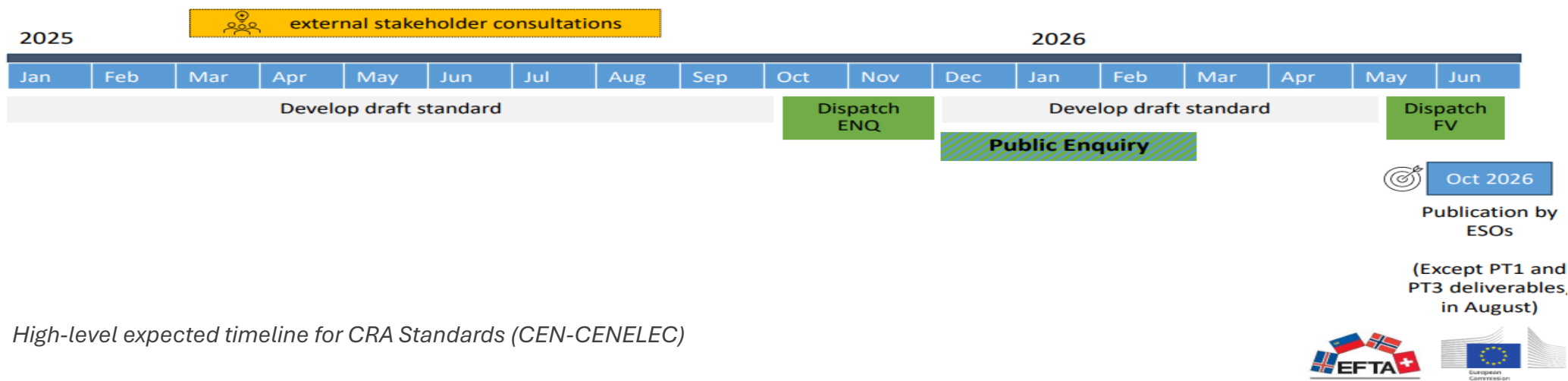
- Hardware devices with security boxes, smart meter gateways, smartcards, etc.
- The EU Commission may require certification according to the Cybersecurity Act (e.g., EUCC) in the future.

- Strictest cybersecurity requirements
- Conformity Assessment: **Third-party conformity assessment** (Modules B+C, H) or European cybersecurity certification scheme (e.g., EUCC)
- Implemented regulation on the Technical description of important and critical products with digital elements (expected Q3 2025)



How are standards relevant for this?

- Standards translate broad legal requirements into concrete, testable technical specifications
- NBs use standards to demonstrate that products, services, or processes comply with relevant EU legislation.
- Standardisation request for CRA standards adopted by EU Commission and notified to European Standardisation Organisations (CEN-CENELEC)
- Harmonised standards grant a 'presumption of conformity'
 - Their use is voluntary
 - Manufacturers can choose another technical solution to demonstrate compliance (e.g., 3rd party conformity assessment)
 - This happens when the EU Commission decides to publish the standard in the Official Journal of the EU



High-level expected timeline for CRA Standards (CEN-CENELEC)

Thank you!

www.tic-council.org

amorenorubio@tic-council.org

+32 487 02 07 32