Co-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 or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Horizontal and Vertical Standards under the Cyber Resilience Act (CRA)CYBERSTAND Specific Service Procedures and STAN4CR Initiatives

Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools

Introduction

- The Cyber Resilience Act (CRA) introduces mandatory cybersecurity requirements for digital products.
- To support compliance, the European standardization system develops harmonized standards.
- These standards define *how* manufacturers, laboratories, and certification bodies can prove that a product is secure.
- They are divided into two main categories — horizontal and vertical standards.

Horizontal Standards

Horizontal standards apply to all products with digital elements, regardless of sector or technology.
They define the baseline cybersecurity principles — such as:

- secure design and default configurations,
- vulnerability handling and updates,
- lifecycle management, and
- transparency of security information.
  They create a foundation for consistency across all products.

Vertical Standards

Vertical standards apply to specific product types or sectors, such as:

- consumer IoT devices,
- industrial control systems,
- semiconductors, or
- medical or automotive systems.

They define sector-specific technical requirements, based on risks, use cases, and operating environments. Together, horizontal and vertical standards create a two-layer model of cybersecurity assurance.

Horizontal and Vertical Layers

- **Horizontal layer** = common cybersecurity principles valid for all.
- **Vertical layer** = detailed requirements for each product category.

Manufacturers must comply with both layers:

- Horizontal standards ensure a consistent baseline of security.
- Vertical standards tailor this baseline to the specific context of the product or industry.

Importance for CRA Compliance

- Compliance with harmonized standards gives **presumption of conformity** under the CRA.
- That means: if a manufacturer follows a relevant horizontal and/or vertical standard, the product is *assumed to meet* the cybersecurity requirements of the Act.
- This reduces administrative burden and ensures mutual recognition of assessments across the EU.

CYBERSTAND – Specific Service Procedures

CYBERSTAND is an EU-funded initiative supporting the development of standards for cybersecurity legislation, including CRA. Through its **Specific Service Procedures (SSPs)**, CYBERSTAND provides:

- funding and expert support for standardization activities,
- coordination between CEN, CENELEC, and ETSI,
- opportunities for experts from labs, academia, and industry to participate in CRA-related standardization.

The 4th SSP specifically focuses on developing standards aligned with CRA.

CYBERSTAND and Horizontal/Vertical Standards

- CYBERSTAND helps develop **horizontal standards** by funding working groups that define common cybersecurity principles.
- It also supports the creation of **vertical standards** for specific sectors, ensuring that these build on the horizontal foundation.
- This approach strengthens coherence and avoids overlapping requirements.

STAN4CR Project Overview

STAN4CR (Standards for Cyber Resilience) is a joint project of CEN, CENELEC, and ETSI. Its goal is to accelerate the development of harmonized standards supporting CRA implementation.

STAN4CR works across two dimensions:

- Horizontal standards (general cybersecurity principles).
- Vertical standards (sector-specific technical details).

It brings together experts from industry, research, and national standardization bodies.

STAN4CR in Practice

STAN4CR technical work focuses on:

- developing horizontal standard *“Principles for Cyber Resilience”*,
- mapping vertical needs for sectors such as IoT, industrial automation, and semiconductors,
- ensuring alignment between European and international standards (ISO/IEC, ETSI).

This ensures that the CRA’s technical implementation is practical and consistent across industries.

Example of Application

Example: A manufacturer of a smart home hub.

- The company applies the horizontal standard “Principles for Cyber Resilience” for basic cybersecurity management.
- It then applies the vertical IoT standard ETSI EN 303 645 for product-specific requirements.
- Testing and certification follow ISO/IEC 17025 and 17065 processes.

The result: a product fully aligned with CRA expectations and ready for EU certification.

Benefits

- Harmonization across all EU markets.
- Easier conformity assessment and reduced duplication.
- Higher trust in cybersecurity certification.

Challenges

- Coordination between horizontal and vertical standards.
- Timely development of sectoral standards.
- Strong participation from SMEs and experts.

Implications for Auditors and Labs

- For auditors and laboratories, understanding both standard layers is essential.
- Horizontal standards define the common assessment principles. Vertical standards provide the specific controls and test methods for each product type.
- Knowledge of ongoing CYBERSTAND and STAN4CR work ensures up-to-date evaluations under CRA.

Next Steps

- Participate in consultations and working groups on CRA-related standards.
- Monitor new horizontal and vertical standards published by CEN, CENELEC, and ETSI.
- Follow updates from CYBERSTAND and STAN4CR websites.
- Align internal procedures and audit criteria with the CRA standardization framework.

Conclusion

- The combination of **horizontal** and **vertical** standards provides a balanced and efficient model for cybersecurity assurance in Europe.
- CYBERSTAND and STAN4CR are central initiatives that make this model operational and practical.
- Together, they enable consistent, measurable, and trusted implementation of the Cyber Resilience Act.

Thank you!

Miroslav Mitev, PhD

+359 896 198 875

m.mitev@dihtrakia.org