PANEL:
HOW TO TRANSLATE CRA IN CSA REQUIREMENTS

Matthias Intemann

BSI, Germany

Head of Certification
Bundesamt für Sicherheit in der Informationstechnik

Martin Schaffer

TIC Council Representative &

SGS

Global Head of
Emerging Technologies

Alexander Eisenberg

BSH Hausgeräte GmbH

Head of Office
EU Technical Market Access

MODERATOR:

Sofia-Roxana BANICA

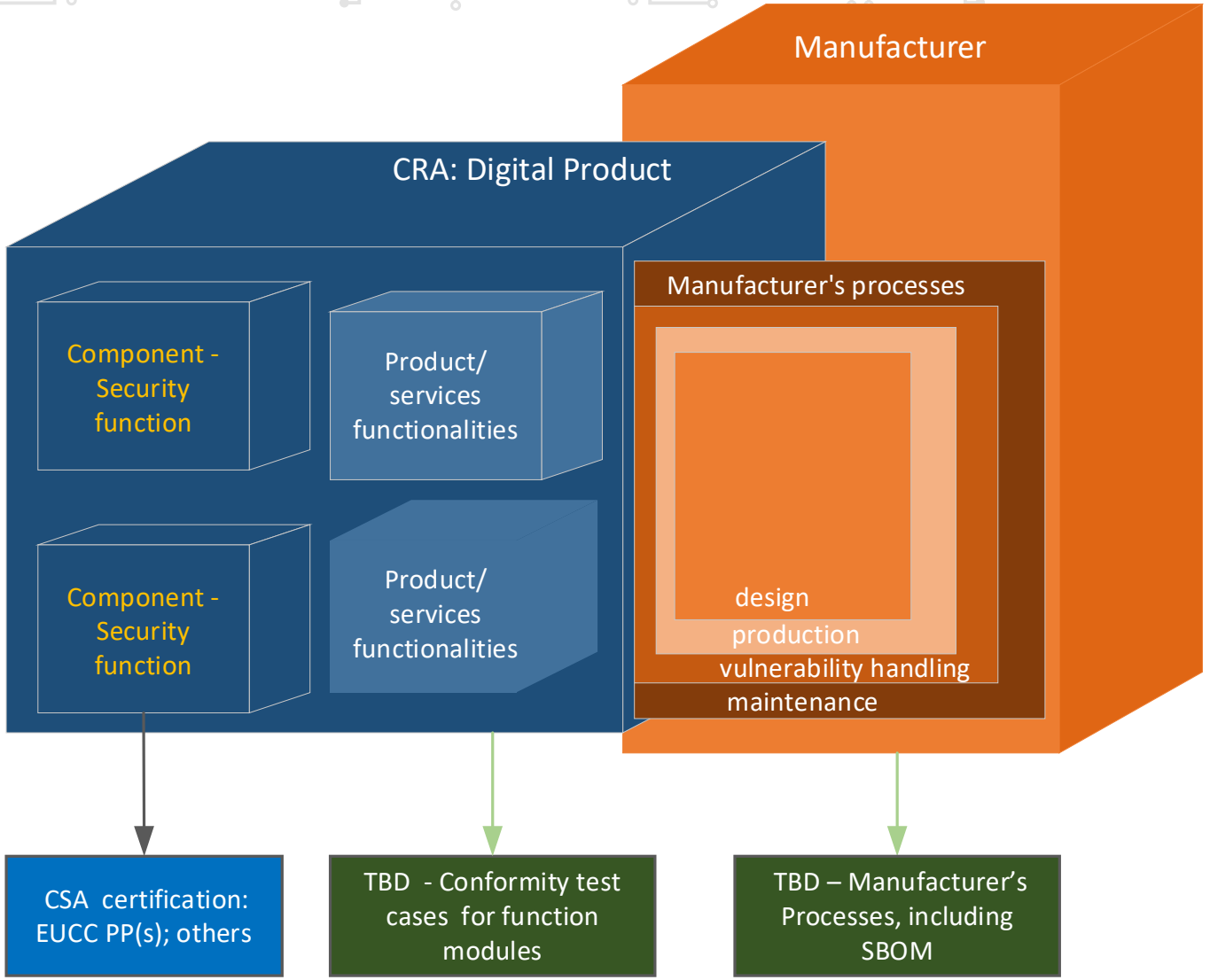
Market, Certification and Standardisation Unit - ENISA

Cybersecurity Officer

THE PANEL OBJECTIVE

Bringing value

Anticipating possible practical alternatives for CRA implementation, based on EU certification schemes and CSA infrastructure for routes to market involving a third-party assessor.



Disclaimer:

All speakers will speak in their own capacity and from their experience accumulated in existing roles, not generating opinions on behalf of the institution they represent.

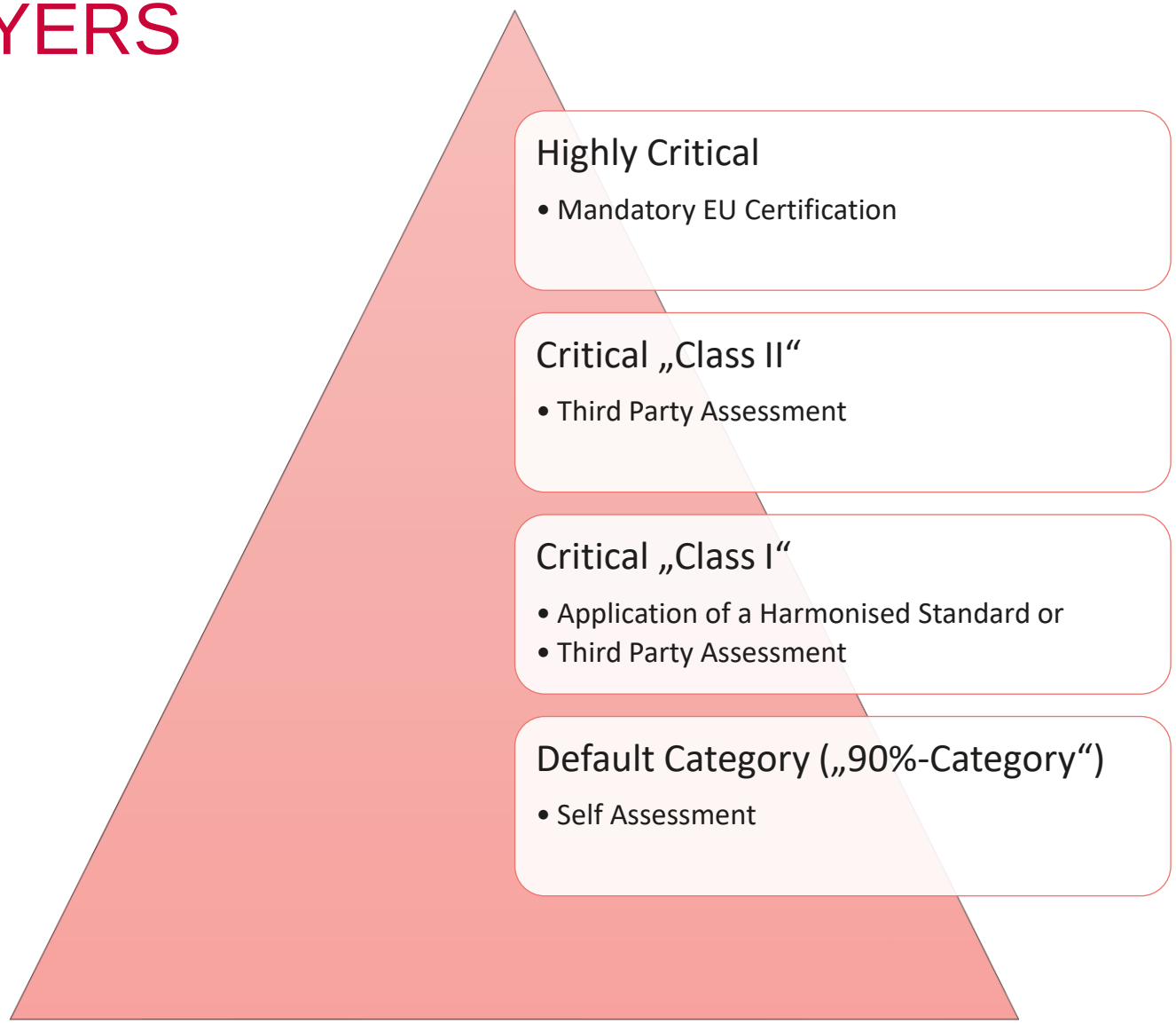
ESSENTIAL REQUIREMENTS OF THE CRA

Security requirements relating to the properties of products with digital elements
- Security-by-design, Security-by-default
- protection from unauthorised access; protection of confidentiality and integrety of data
- designed, developed and produced to limit attack surfaces [...]

Vulnerability management
- SBOM at the very least of the top-level dependencies of the product;
- Address and remediate vulnerabilities without delay, including by providing security updates
- Public disclosure of information about fixed vulnerabilities, information allowing users to identify the product [...]

Minimum information for the user
- Contact information where cybersecurity vulnerabilities of the product can be reported and received
- Identification of product
- Possibility to asses conformity information and if made available SBOM [...]

THE CRA LAYERS



NLF CONFORMITY MODULES (DECISION 768/2008/EC)

A

- A: Internal production control
- A1: Internal production control plus supervised product testing
- A2: Internal production control plus supervised product checks at random intervals

CRA

B

- B: EC-type examination

CRA

C

- C: Conformity to type based on internal production control
- C1: Conformity to type based on internal production control plus supervised product testing
- C2: Conformity to type based on internal production control plus supervised product checks at random intervals

CRA

D

- D: Conformity to EC-type based on quality assurance of the production process
- D1: Quality assurance of the production process

E

- E: Conformity to EC-type based on product quality assurance
- E1: Quality assurance of final product inspection and testing

F

- F: Conformity to EC-type based on product verification
- F1: Conformity based on product verification

G

- G: Conformity based on unit verification

H

- H: Conformity based on full quality assurance
- H1: Conformity based on full quality assurance plus design examination

CRA

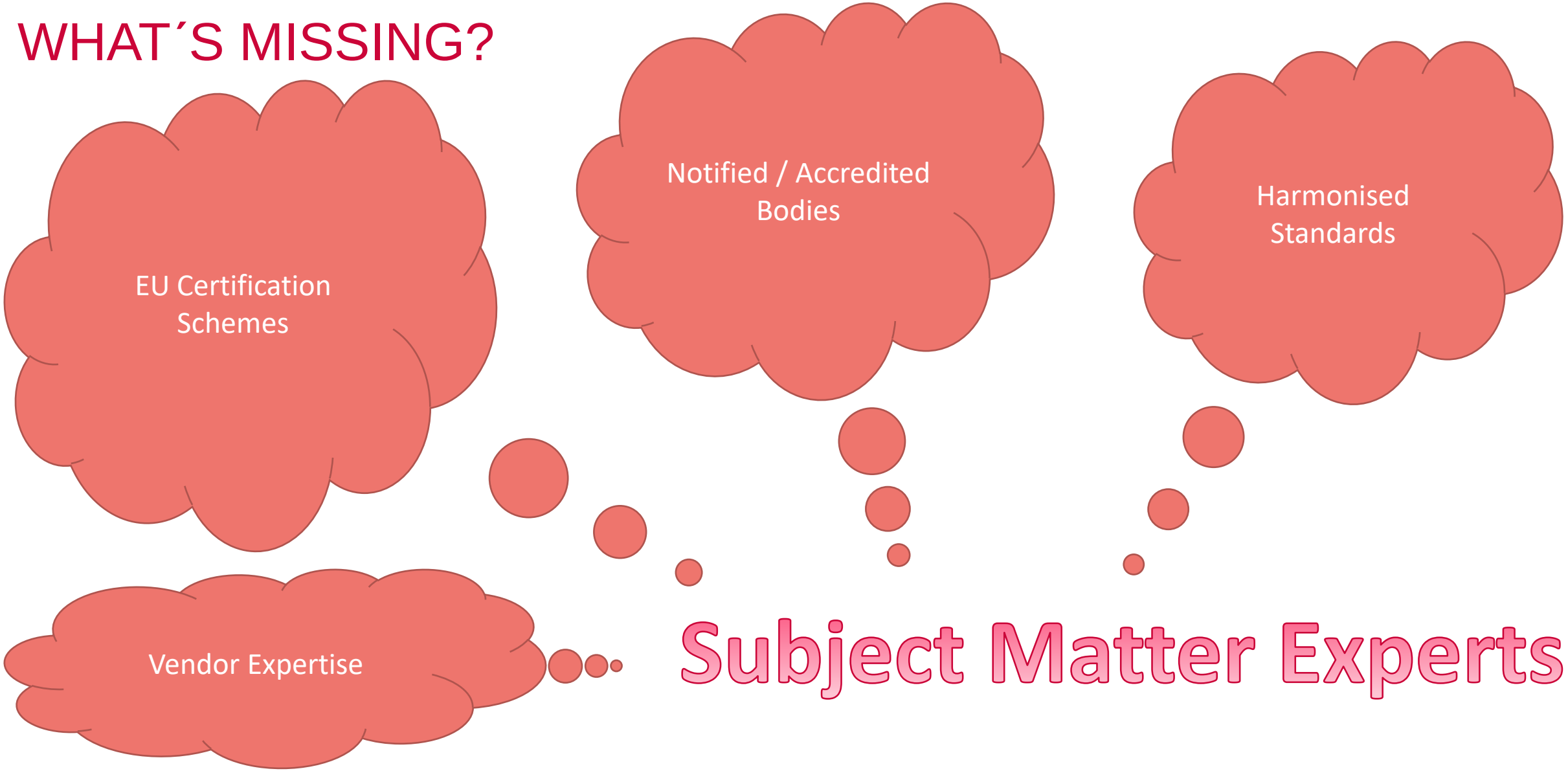
CRA Virtual Module

I

- I: CSA EU scheme certification

CRA

WHAT´S MISSING?



THE SOLUTION?

Default

ENISA to foster best practice exchange

Interim Checklist to fulfil Essential Requirements

Critical I & II

Make use of existing CSA CAB infrastructure

CSA/CRA Conformity Modules Supplement EU Schemes with Gap focused Activities

Iterative approach on developing Harmonised Standards

Highly Critical

Build generic CSA/CRA Conformity Modules based on Essential Requirements

Re-Use existing Sets of sectorial requirements (e.g. Protection Profiles)

TAKEAWAY:

[Member State Representative in its role of NCCA]

"IT security is essential to the EU's prosperity and overall security. With hardly any EU harmonisation in place, the task of CRA implementation is demanding on all involved parties. Modularisation and flexible usage of standards, conformity assessments (NLF/CSA), and accreditations are key to success." Matthias Intemann

[Manufacturer of Consumer Products]

"Coherence between CRA and CSA is of paramount importance for effective EU cybersecurity regulation of products. However, CSA schemes and CRA requirements may end up diverging, as their process to be developed is different. International and European standards should be the connecting link between CSA schemes and CRA requirements.
Furthermore, CSA schemes should be developed under the same conditions as ESO standards, namely openness to all interested parties, consensus and transparency (see Annex II of Regulation 1025/2012)." Alexander Eisenberg

[TIC Council Representative: representing independent testing, inspection and certification companies]

"Across cybersecurity regulations, harmony, breadth, and flexibility on the what and the how are crucial for involved stakeholders. A risk-based framework allows customization, yet we must be cautious with pre-defined risk mappings. The focus shouldn't be solely on intended use cases - low-risk assumptions, like with consumer IoT devices, can be misleading. Risks, as shown by bot-net attacks, often lurk in the least expected places." Martin Schaffer