Openforum europe
open, competitive choice for IT users

Some Proposals around the Draft Regulation on the Cybersecurity Act

Learning from the New Legislative Framework / New Approach

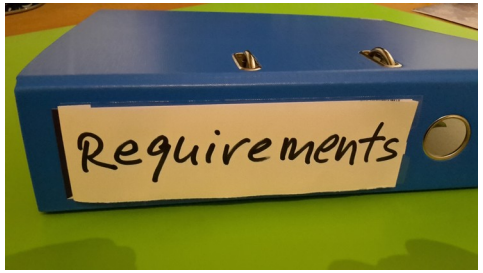
Standards – Self-assessment – Risk Management

Dr. Jochen Friedrich
Chair of the OFE Standardisation Task Force

Brussels,13 February 2018

Standards and Certification

REQUIREMENTS



Essential requirements which need to be met

Developed in close interaction with stakeholders

step one

Compliance << Implementation

STANDARD

Methods / processes how to meet the essential requirements

Developed in SDO – open; broad consensus

step two

Available for planning and implementation

CERTIFICATION

Assessment that standard is properly implemented and that requirements are met

step three

Confirmation that requirements are fulfilled

"Toolbox" of what is applied in the EU New Legislative Framework (NLF)

From Certification Schemes to Certification

European Commission:
- Initiate process

ENISA:
- Develop scheme (requirements, identification of standards, ...)
- Consultation with and involvement of **EU Multistakeholder Platform on ICT Standardisation (MSP)**

European Commission:
- Adopt scheme following comitology procedure

Industry:
- Implement standards as identified in the respective scheme

European Commission:
- If needed: Initiate standardisation request to **ESOs**

ESOs and other SDOs
- Have already effective cybersecurity standards in portfolio and set up infrastructure for effective further work

EITHER:
- 3rd party assessment and certification

OR:
- Self-assessment

Accredited bodies:
- Make use of available infrastructure as much as possible

Market surveillance

step one

step two

step three

"Toolbox" of what is applied in the EU New Legislative Framework (NLF)

Self-Assessment is a Full-Fledged Process

Regulation 765/2008

Article 30 – General principles for CE Marking

§

1. The CE marking shall be affixed only by the manufacturer or his authorised representative.

[…]

3. By affixing or having affixed the CE marking, the manufacturer indicates that he takes responsibility for the conformity of the product with all applicable requirements set out in the relevant Community harmonisation legislation providing for its affixing.

4. The CE marking shall be the only marking which attests the conformity of the product with the applicable requirements of the relevant Community harmonisation legislation providing for its affixing. […]

Self-assessment is not a lower level assurance of conformity but equal to 3rd party assessment

Via the NLF a framework of in-house test labs etc. is available that should be eligible to be used for cybersecurity as well

"Toolbox" from NLF is well established and well proven

"Toolbox" of what is applied in the EU New Legislative Framework (NLF)

Risk Management instead of Assurance Levels

CURRENT PROPOSAL

Three assurance levels:

(i) basic
= limited confidence

(ii) substantial
= substantial confidence

(iii) high
= high confidence

Issues:

- **! Lack of clarity**
- **! Confusion**
- **! High cost**
- **! Little benefit**

RISK MANAGEMENT APPROACH

Prioritisation of risk profiles appropriate to context

Essential Requirements defined

Standard meets respective requirements

Certify against appropriate standard

NB: Common Criteria are also moving away from Example Assurance Levels in favour of scheme specific requirements

Benefits:

- **! Increased Clarity & Effectiveness**
- **! Broadly accepted**
- **! Market-based incentives**
- **! Cost-benefits balance**

one-dimentisonal approach

clearly prioritised risk management instead

Voluntary – Mandatory

if

the Regulation is about voluntary certification only this should be very clear and use in mandatory contexts (Union Acts) should be excluded

but if

the Regulation may be envisaging mandatory cybersecurity certification

this constitutes a market access requirement and therefore

the New Legislative Framework / New Approach should be applied

and

double certification – one process for NLF regulation, one for cybersecurity certification – should be avoided