



Supporting European (SMEs) participation in the standardisation process

SMEs in a multi-standards “digital” world:
Critical factor for Digital Single Market & Industry 4.0 (5.0)

Dr. George Sharkov, European Digital SME Alliance & SBS

Director, European Software Institute Center Eastern Europe
Head, Cyber Security and Resilience Lab



About us



Europe's first and largest ICT SMEs association

30 members (associations)

Representing more than 20,000 digital SMEs across Europe

- Represent the interests of SMEs in the standardisation process (CEN, CENELEC, ETSI, ISO & IEC)
- Raise awareness of SMEs for standardisation
- Motivate SMEs to become involved in the standardisation process

Political

- Member of the governing bodies of the ESOs
- Observer in the EC Committee of Standards
- Follow-up & comment on policies related to standardisation

Technical

- 60 experts in > 200 TCs/WGs approx. 20 sectors
- Participation in TCs, WGs to ensure SME-compatible standards
- Participation in ESOs Technical Boards

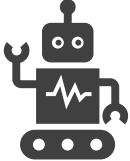
SBS members



Digital SMEs – roles and expertise



B2B software solution providers



Industrial AI developers

DIGITAL ENABLERS



data- and IoT-specialised SMEs



IT consultants

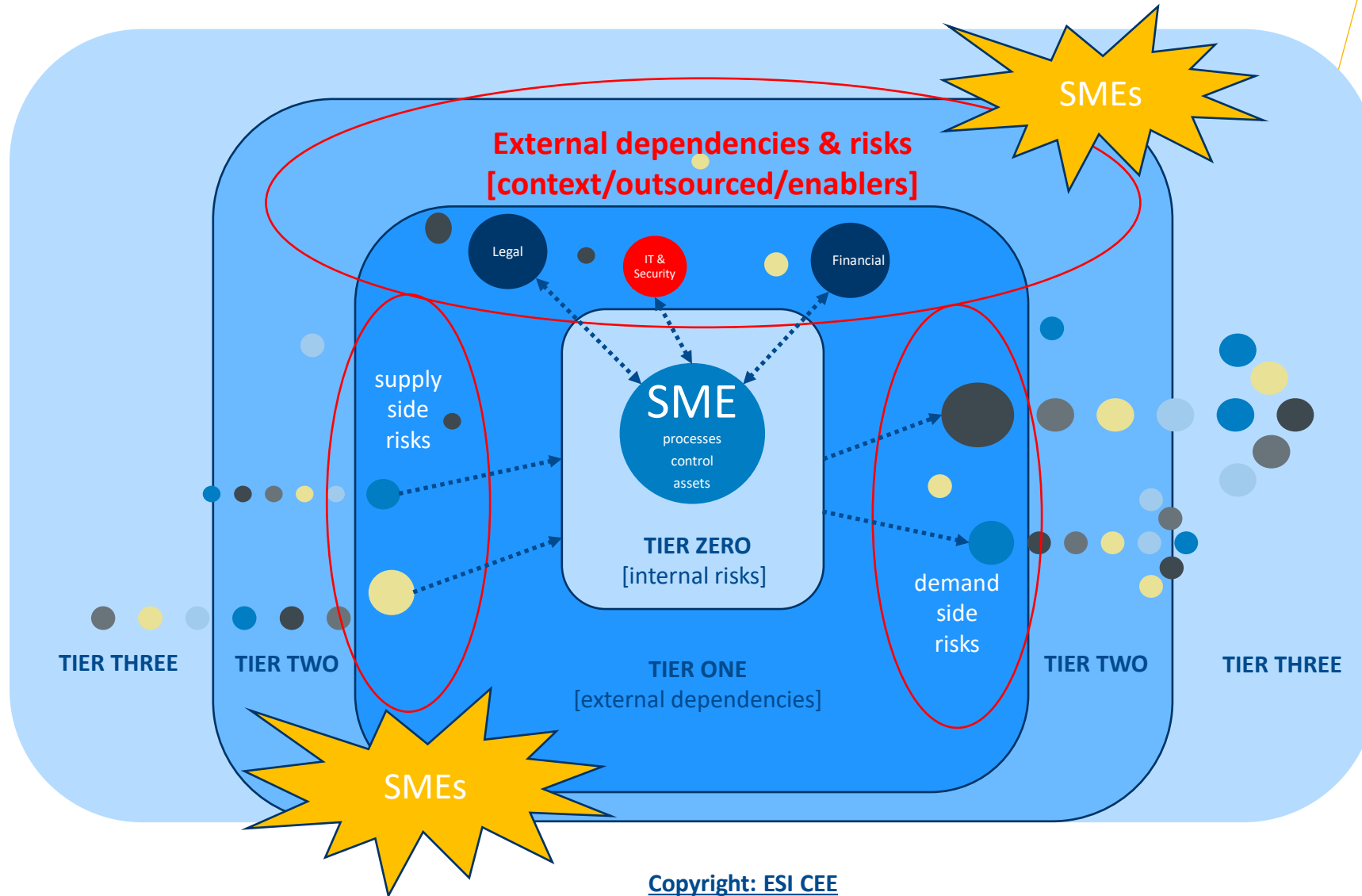


IT security providers

CSA implementation and SMEs:

SMEs represent a vast majority of after-sales servicing and support companies

SMEs in supply/value chains - hidden threats?



1) **TRUST** = Need standards applicable and affordable for ALL players (SMEs!!)

2) Provide **engagement** and **propagation** mechanism (shared risk requires shared responsibility)

Example
NotPetya spread over Supply Chains and affected the global net



SMEs & ICT Standardisation Participation



- SMEs and association representatives of the ICT sector
- SBS members and experts (all sectors)
- Secretariat: DIGITAL SME



EUROPEAN STANDARDS ORGANIZATIONS



Overview of Standardisation Activities

- Task Forces – Standards Implementation guides
 - SBS SME Guide on Information Security Management (2017)
 - SBS SME Guide on IIoT (2020)
 - SBS SME Guide on Information Security Controls (2021)
- SBS Position papers
 - [eIDAS Regulation: Strengthening SMEs through standardisation](#) (2020)
 - [The EU Cybersecurity Act and the Role of Standards for SMEs](#) (2019)
 - [Radio Equipment Directive: Software can be one of Europe's strongest economic sectors. Can EU laws support it better?](#) (2019)
 - [SBS position on cybersecurity solutions and certification for SME users and providers of critical services](#) (2018)
 - [SBS position paper on Standards Essential Patents, a new EU approach: what is at stake for SMEs?](#) (2018)



SME Implementation Guides



Help digital and non-digital SMEs implement ICT standards to enhance their business processes and strengthen their operations



Ongoing work:

1. Updating the SBS SME Guide for the implementation of ISO/IEC 27001 on information security management - Expected Q3/2021
2. Developing a new SME Guide on Information Security Controls ISO/IEC 27002 - Expected Q3/2021

Overview of Standardisation activities

SBS ICT Forum

- [SBS ICT Forum 2020 – Policy, Norms & Standardisation of Artificial Intelligence: Challenges and Opportunities for SMEs](#) (2020)
- [SBS ICT Forum 2019: SMEs, Standards, and the EU Cybersecurity Act](#) (2019)
- [SBS Forum on ICT standardisation: Open standards in ICT procurement](#) (2018)
- [Forum on ICT standards for SMEs: e-invoicing and e-identification](#) (2017)
- [Forum on ICT standards: SMEs to become standards setters!](#) (2016)



SBS SME Compatibility Test for Standards



Provide an overall perception of the SME compatibility of any given standard



Based on CEN-CENELEC Guide 17



Rank into broad categories (good, average and poor standards)



Starting point for possible improvement of standards



To be updated in line with users' experiences



SME Compatibility test- Composition & use



- Intended for people with **some experience in standardisation & the subject area**
- Can be applied at any stage of development: Enquiry, Formal vote, finalised standards and on any standard (national, EN, International)
- Online form with questions calculating overall score
 - 11 criteria and 21 questions
 - Related to **text** of standard & **impact/implementation**
- Scores: 1,3,5, N/A (non-applicable)
- Different **weight of different criteria**

A screenshot of a web form titled 'SME Compatibility Test for Standards'. The form is for 'CRITERION 1: JUSTIFICATION, TARGET GROUP AND RELATION WITH OTHER STANDARDS'. It contains introductory text explaining the purpose of the test and the importance of providing accurate information. Below this, there is a question: '1.1 Are relations to other standards and main changes to previous editions appropriately indicated?'. There are four radio button options: 'Score 1 - There is insufficient information missing. For scores 2 to 5, the most important changes to the previous edition for the case of revisions or issuing standards are not fully or relevant information on the relation with other standards is not included i.e. whether the standard replaces another document completely or in part or whether it is intended to be used with another standard'; 'Score 2 - There is some information, but the information is incomplete or unclear'; 'Score 3 - The information is correct, complete and clear'; and 'Not applicable'. At the bottom, there is a text box labeled 'Supporting evidence'.

SBS SME Compatibility test - Criteria

- ✓ Justification, target group and relation with other standards (3 Q.)
- ✓ Scope (1 Q.)
- ✓ Normative references (1 Q.)
- ✓ Market access (1 Q.)
- ✓ Relevance of the content (1 Q.)
- ✓ Cost (requirements) & conformity assessment (4 Q.)

- ✓ Readability (1 Q.)
- ✓ Availability of guidance (1 Q.)
- ✓ Necessary modifications before applying the standard (3 Q.)
- ✓ Availability of external elements for implementation (4 Q.)
- ✓ Appropriate transition period (1 Q.)



SME Compatibility test – Criteria/Questions



Market access (1 Q.)

Market access considers whether any requirement or defined performance level has the effect of forcing some products off the market or preventing current practices. In some cases, this could be justified because of safety or legal requirements. Nevertheless, in other cases this could create unjustified barriers or particularly affect SMEs. This could for example be because the provisions of the standard (for example a specific test method selected)

Question 4.1: Does the standard prevent (implicitly or explicitly) some products or services from accessing the market or the use of specific technologies?

Cost (requirements) & conformity assessment (4 Q.)

Perhaps one of the most important criteria of the assessment method. It addresses the cost and difficulty associated with applying any standard, identifies whether requirements are imposed unnecessarily, whether assessment methods are reasonable or whether the standard offers simplifying options. It also looks at whether the standard respects the neutrality principle regarding conformity assessment and does not for example impose third party certification.

Question 6.1 Does the standard impose unnecessary requirements?

Question 6.2: Are justified requirements assessed by burdensome methods?

Question 6.3: The frequencies of assessment are?

Question 6.4: Does the standard respect the neutrality principle regarding conformity assessment?

The neutrality principle requires that all standards shall be written in a way such that conformity with the specified requirements can be assessed by a manufacturer or supplier (first party), a user or purchaser (second party), or an independent body (third party).

SME Compatibility test – scoring



0 - 33%

The standard is **poor** & causes substantial challenges for SMEs. It requires urgent/fundamental improvement.



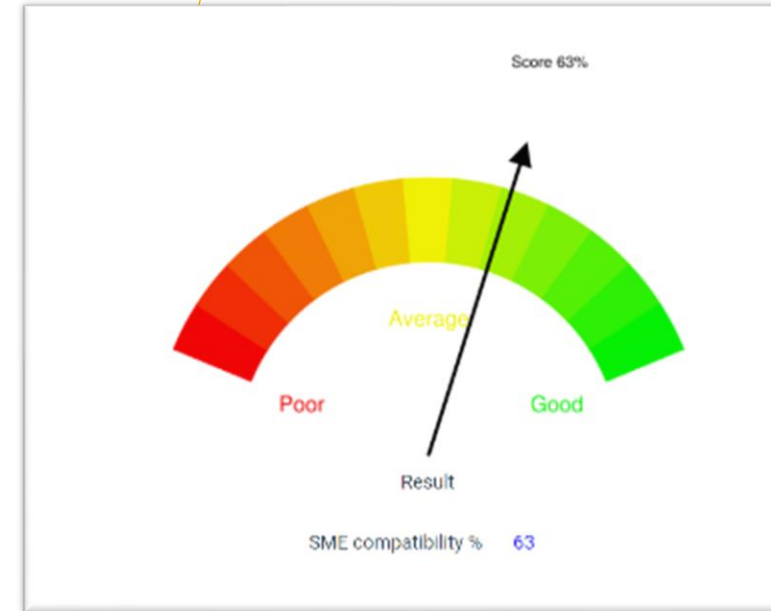
34 - 66%

The standard is **average** in relation to compatibility with SME's needs. It should be improved.



67 - 100%

The standard is **good** & compatible with SMEs' needs in general. It requires little or no change



SME Compatibility Test - Pilot Results



Examples:

ETSI TS 103 645 / ETSI EN 303 645 (TC CYBER)
"CYBER: Cyber Security for Consumer Internet of Things: Baseline Requirements", Version 2.08, 2020-04

SME compatibility **85 %**



<https://www.sbs-sme.eu/sme-compatibility-test-standards>

25 valid tests performed so far:

- National, International and European deliverables (TS, IWA, ENs...)
- Various sectors: furniture, glass, bikes, road vehicles, toys, ergonomics, switchgear, quality management.....
- Pilot test of ETSI TC CYBER (TS 103 645)
- Two standards identified as rather poor (38% and 45%)
- Presented at ETSI TC CYBER#25 & ETSI Security Week 2021

SMEs & standards - EU CSA, NISD & NISD-2, Directive on Resilience of Critical Entities,...



[based on the joint Position Paper SBS&DSME Alliance, 2019]

Types of SMEs:

- ‘digital enablers’: developing and providing digital hardware, software and services, incl. after-sales support and servicing
- ‘digitally based’ SMEs – strongly connected to first group, clusters, value-chain, outsourcing, incl. cloud-services
- ‘digitally dependent’ SMEs – the backbone of the digital economy
- digital/digitized ‘start-ups’

Principles:

- “Size does matter” - (external) dependability and maturity level of the company are cross-parameters – “small is BIG”
- **Differentiation** is needed to tailor standards and certification schemes to different **types and sizes of SMEs**

Standards and SMEs – the Four “A”-challenges

- **Affordability (Accessibility)**: Standards are not always freely available, and implementation is expensive
- **Adaptation**: Standards are not tailored to SMEs and there are no easy technical solutions or guides for implementation
- **Awareness** and internal organizational capability (knowledge-skills-competences)

Good practice: From Lightweight Cybersecurity Assessment to SME Certification Scheme (in Belgium)



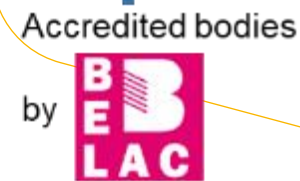
inspired/aligned
scaled down

**"Keep IT Secure" (KIS)
2018**

Digital Wallonia

Center for Cybersecurity
Belgium

<https://www.digitalwallonia.be/fr/publications/keepitsecure>



SMEs and new technologies: EU AI Strategy & AI Act

Legal Framework on AI, risk-based, conformity assessments



Regulatory sandboxes Art. 53 and 54



- ✓ **National authorities** in charge of individual schemes, cross-border sandboxes possible
- ✓ Uniform **common principles** and criteria
- ✓ **Cooperation** between MS and a future AI Board to ensure common European approach
- ✓ Further processing of personal data in the public interest in the sandboxes

Support for SMEs/start-ups Art. 55



- ✓ **Priority access to regulatory sandboxes for SMEs and start-ups**
- ✓ **Support SMEs viability: specific consideration of small-scale providers, with regard to certain obligations and conformity assessment fees.**
- ✓ **Harmonised technical standards to help small providers demonstrate compliance**

The "new" digital world (and security):

- AI/ML
- Autonomous / robotics
- Cyber/Physical
- Big Data
- Quantum
- Space

Standards + Requirements +
Certification schemes

Upbuilding, not Overbuilding

e.g. "triple helix" integrated
approach (strategies):
AI + cybersecurity + IIoT

Conclusions

- Standards / Certification Schemes shall cover SMEs - the four “A” for SMEs – **Affordable (Accessible), Adapted, Aware (Adopted)**
- **Lightweight (also self-assessment, conformity declarations)** should be “including” (encouraging) for SMEs to go for certification (higher levels, like with **capability-maturity levels**)
- Mind the SMEs when migrating/transiting **from National to EU-wide certification schemes**
- Consider “**SME Compatibility Test**” for Cybersecurity Certification Schemes (as an implementation KPI)
- SMEs are essential (and critical) parts of the supply/value chain, including third-party services (“hidden threats”) – propagate requirements (standards, certifications) throughout all the branches of the chain
- Digital SMEs represent a **vast majority of after-sales servicing and support companies** (including IT-security aspects) – focus on resiliency
- “New digital world” – gradually build standards + certification schemes - apply harmonized (technical) standards approach to help small providers demonstrate compliance, and **avoid multi-standards burden**



small is BIG

Further Questions?

Contact me:

Dr. George Sharkov, representing SBS in ETSI TC CYBER, ISG SAI & ENISA SCCG

gesha@esicenter.bg