WE
CAN DO
SO MUCH
TOGETHER

Where is the EU in cloud security certification?: Main findings

Certification schemes for cloud computing
SMART 2016 / 0029

Leire Orue-Echevarria
TECNALIA

December 11th, 2017

tecnalia Inspiring Business

Agenda

01 Context

02 Approach

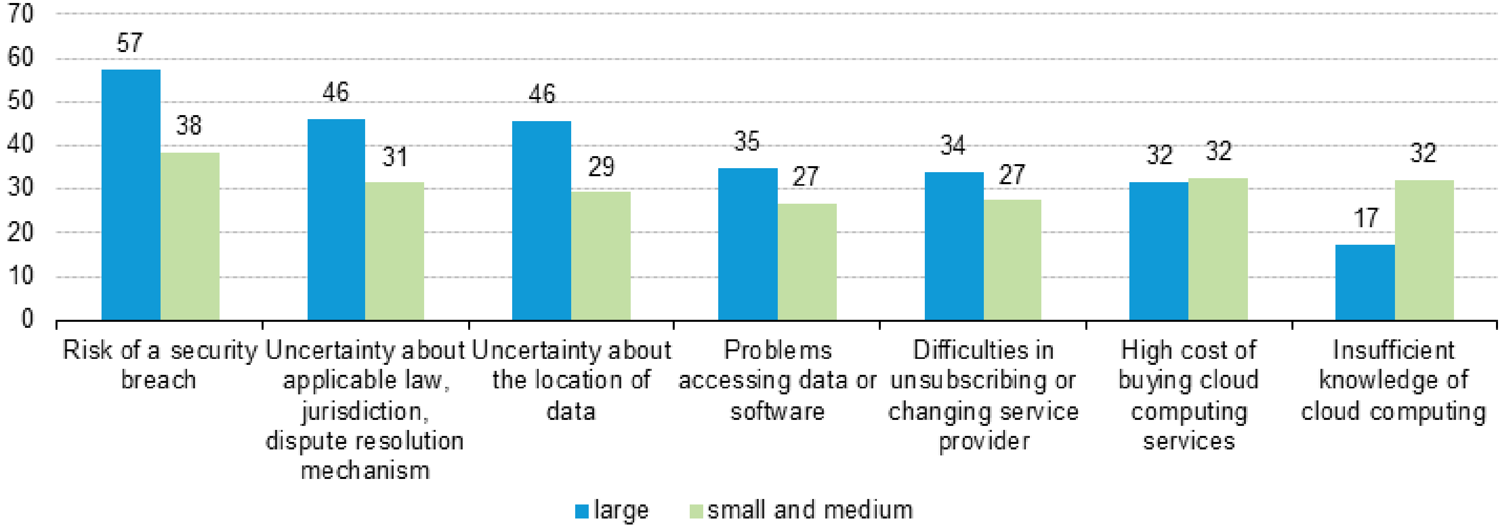
03 Stakeholders analysis

04 Market adoption

05 Next steps

01 Context and Motivation

- What is limiting enterprises from using cloud computing services?



Factors limiting enterprises from using cloud computing services, by size class, EU-28, 2014 (*)

- This can be extended to the Public Sector

(*) Source: Eurostat, 2014

01 Context

- Customers need to know and be **assured** that their **data** is **equally safe** no matter where they are located or who provides the service
  - What security aspects need to be considered in cloud computing that ensure Free Flow of Data and cross-border?
  - What regulation aspects need to be considered / addressed?
- What should be the role of the EC?

01 Context

- Plethora of standards, schemes and other relevant frameworks

ISO/IEC 17203, ISO/IEC 17826:2012, ISO/IEC 19041, ISO/IEC 19044, ISO 19086, ISO/IEC 19099, ISO/IEC 19831, ISO 19941, ISO 19944, ISO/IEC 20000-1, ISO 22301,ISO/IEC 24760-1, Family of ISO/IEC 2700x, ISO/IEC 29100, ISO/IEC 29101, ISO/IEC 29115.

NIST SP 500-299, Draft NIST SP 500-307, NIST SP 800-125, NIST SP 800-144 NIST 800 - 53

OASIS TOSCA, OASIS CAMP

SNIA CDMI, DMTF DSP0243, DMTF DSP0263

CSA CCM, CSA Star, CSA PLA, CSA Attestation - OCF Level 2, CSA Attestation - OCF Level 1, CSA Self-Assessment - OCF Level 1

ITU-T X.1601, ITU-T X.1631

Others

AICPA SOC 1, AICPA SOC 2, AICPA SOC 3

Agenda

01 Context

02 Approach

03 Stakeholders analysis

04 Market adoption

05 Next steps

02 Approach

Standards Frameworks Schemes

Public Initiatives

Private - Public Initiatives

Stakeholders Analysis

Market Adoption

Policy (see next presentation)

02 Approach

Standards Frameworks Schemes

Public Initiatives

Private - Public Initiatives

Stakeholders Analysis

Market Adoption

Policy (see next presentation)

02 Approach

	ISO 17203	ISO 17789	ISO 19944	ISO 19941	ISO 19086	ISO 19099	ISO 22301	ISO/IEC 24760	Family of 27000 ISO/IEC 27000 , ISO/IEC 27001 & ISO /IEC 27002	ISOIEC 29100	ISO/IEC 29101	ISO/IEC 29115
1. Information security policy	🟥	🟨	🟥	🟩	🟩	🟥	🟨	🟨	🟩	🟨	🟨	🟨
2. Risk management	🟥	🟨	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩
3. Security roles	🟥	🟥	🟥	🟩	🟩	🟥	🟩	🟩	🟩	🟩	🟩	🟩
4. Security in Supplier relationships	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟩	🟥	🟥	🟥
5. Background checks	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟩	🟥	🟥	🟥
6. Security knowledge and training	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟩	🟥	🟥	🟥
7. Personnel changes	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟥	🟥
8. Physical and environmental security	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟥	🟨
9. Security of supporting utilities	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟩	🟥	🟥	🟥
10. Access control to network and information systems	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟩	🟩	🟩	🟥
11. Integrity of network and information systems	🟥	🟨	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟥	🟥
12. Operating procedures	🟥	🟨	🟥	🟨	🟥	🟥	🟩	🟥	🟩	🟥	🟥	🟥
13. Change management	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟩	🟥	🟥	🟥
14. Asset management	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟥	🟥
15. Security incident detection and response	🟥	🟨	🟥	🟥	🟨	🟥	🟩	🟥	🟩	🟥	🟥	🟥
16. Security incident reporting	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟩	🟥	🟥	🟥
17. Business continuity	🟥	🟨	🟥	🟨	🟨	🟥	🟩	🟥	🟩	🟥	🟥	🟥
18. Disaster recovery capabilities	🟥	🟨	🟥	🟥	🟩	🟥	🟩	🟥	🟩	🟥	🟥	🟥
19. Monitoring and logging policies	🟥	🟨	🟥	🟥	🟥	🟥	🟩	🟥	🟩	🟥	🟥	🟥
20. System tests	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟩	🟥	🟥	🟥
21. Security assessments	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟥	🟩	🟥	🟥	🟥
22. Checking compliance	🟥	🟨	🟥	🟥	🟨	🟥	🟩	🟥	🟩	🟥	🟥	🟥
23. Cloud data security	🟥	🟥	🟥	🟥	🟨	🟥	🟨	🟥	🟩	🟥	🟥	🟥
24. Cloud interface security	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟥	🟩	🟥	🟥	🟥
25. Cloud software security	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟥	🟩	🟥	🟥	🟥
26. Cloud interoperability and portability	🟥	🟥	🟥	🟩	🟥	🟥	🟥	🟥	🟥			🟥
27. Cloud monitoring and log access	🟥	🟨	🟥	🟥	🟥	🟥	🟥	🟥	🟩			🟥

🟥	Not covered
🟨	Partially covered
🟩	Fully covered

02 Approach

- Available standards tackle many issues that require to go through different certification / attestation processes
- The depth in which security aspects are covered varies depending on the standard

02 Approach

Standards Frameworks Schemes

Public Initiatives

Private - Public Initiatives

Stakeholders Analysis

Market Adoption

Policy (see next presentation)

02 Approach

- Analyzed strategies from the governments of Spain, Italy, Germany, France, Latvia

DE – C5 catalogue

- 17 control areas
- Per each control: Objective, requirement (basic, additional)
- Attestation
- No certificate,
- Relies on int’l standards
- Cloud-specific

ES - ENS

- For eAdmin CSP / digital providers
- Dedicated regulation for cloud issues, providers or not of the eAdmin
- Systems have categories: low, medium, high
    - Low=self assessment
    - Medium/high= audit every 2 years
- Audit

FR - SecNumCloud

- Certification for CSPs
- Based on ANSSI recommendations and int’l standards
- 2 levels: basic and advanced (^)
- Label

IT - PM Decree 2013

- National ICT security certification scheme based on int’l standards,
- no cloud-specific

(^) Requirements for ‘Advanced’ are as of 08.09.2017 not published

02 Approach

- Different maturity levels of public sector initiatives in EU28
- Different approaches: from market driven to highly regulated scenarios
- Different levels of granularity
- Harmonisation at EU level is considered necessary

02 Approach

Standards Frameworks Schemes

Public Initiatives

Private - Public Initiatives

Stakeholders Analysis

Market Adoption

Policy (see next presentation)

02 Approach

- Analyzed (cross-border) public-private initiatives: Trusted Cloud, Label Cloud, ESCloud, Zeker Online

Trusted Cloud

- German initiative, now onto FR and NL
- Non-profit association
- For SMEs, both CSPs and cloud users
- Own criteria catalogue
- Legally bound self-assessment

Zeker Online

- 2 pillars: legal and infrastructure
- covers the whole service stack
- Based on standards
- Audit

Label Cloud

- Initiative by France IT
- For SMEs
- 3 layers (IaaS, PaaS, SaaS)
- 3 levels: initial, confirmed, expert
- Based on NIST and ITIL
- Label for 2 (initial), 3 (confirmed), 4 (expert) years
- Continuous improvement, so recertification obliges to obtain better results than the previous time

ESCloud

- Collaboration of France and Germany
- Label
- 15 core principles
- No mutual recognition between SecNumCloud and C5

02 Approach

- Cross-border efforts are commendable
- However, mutual recognition is still not sufficiently addressed
- Duplication of efforts?

Agenda

01 Context

02 Approach

03 Stakeholders analysis

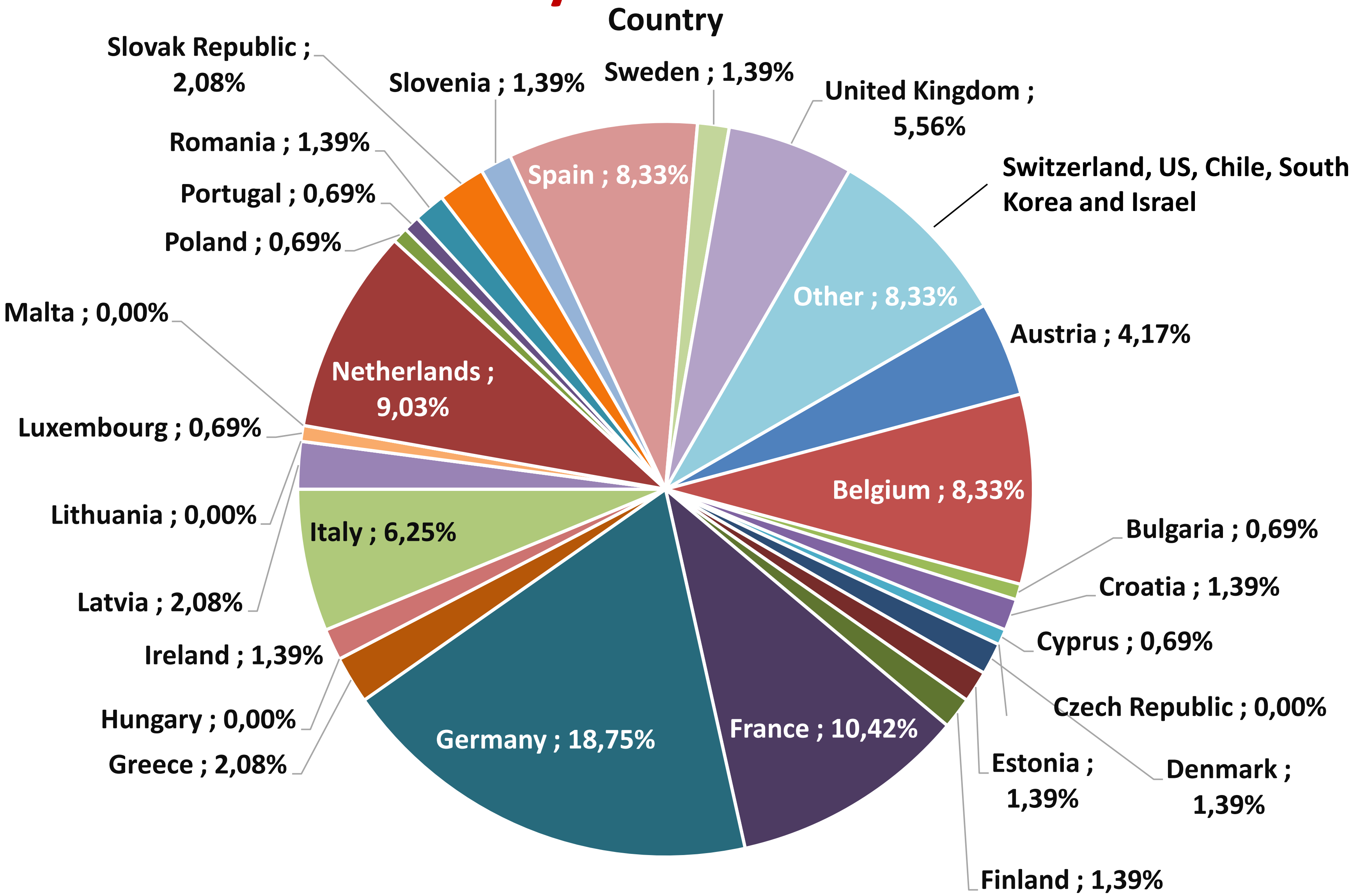
04 Market adoption

05 Next steps

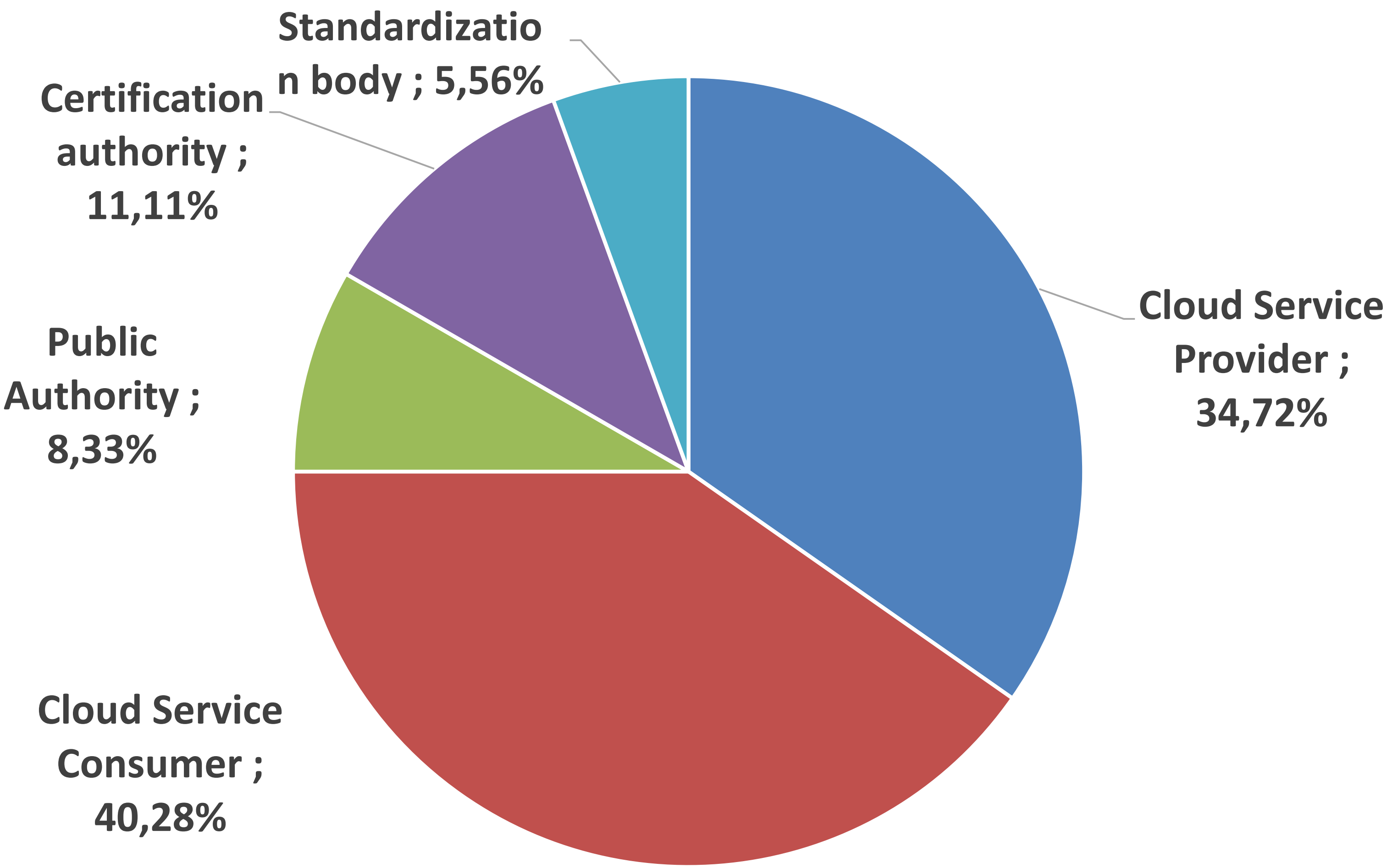
03 Stakeholders analysis

- Survey: 28.09.2017 – 15.11.2017
- Reopened and accessible through: http://tinyurl.com/cloudcertification
- 494 respondents but only 200 answers were 100% complete, which have been retained for analysis

03 Stakeholders analysis



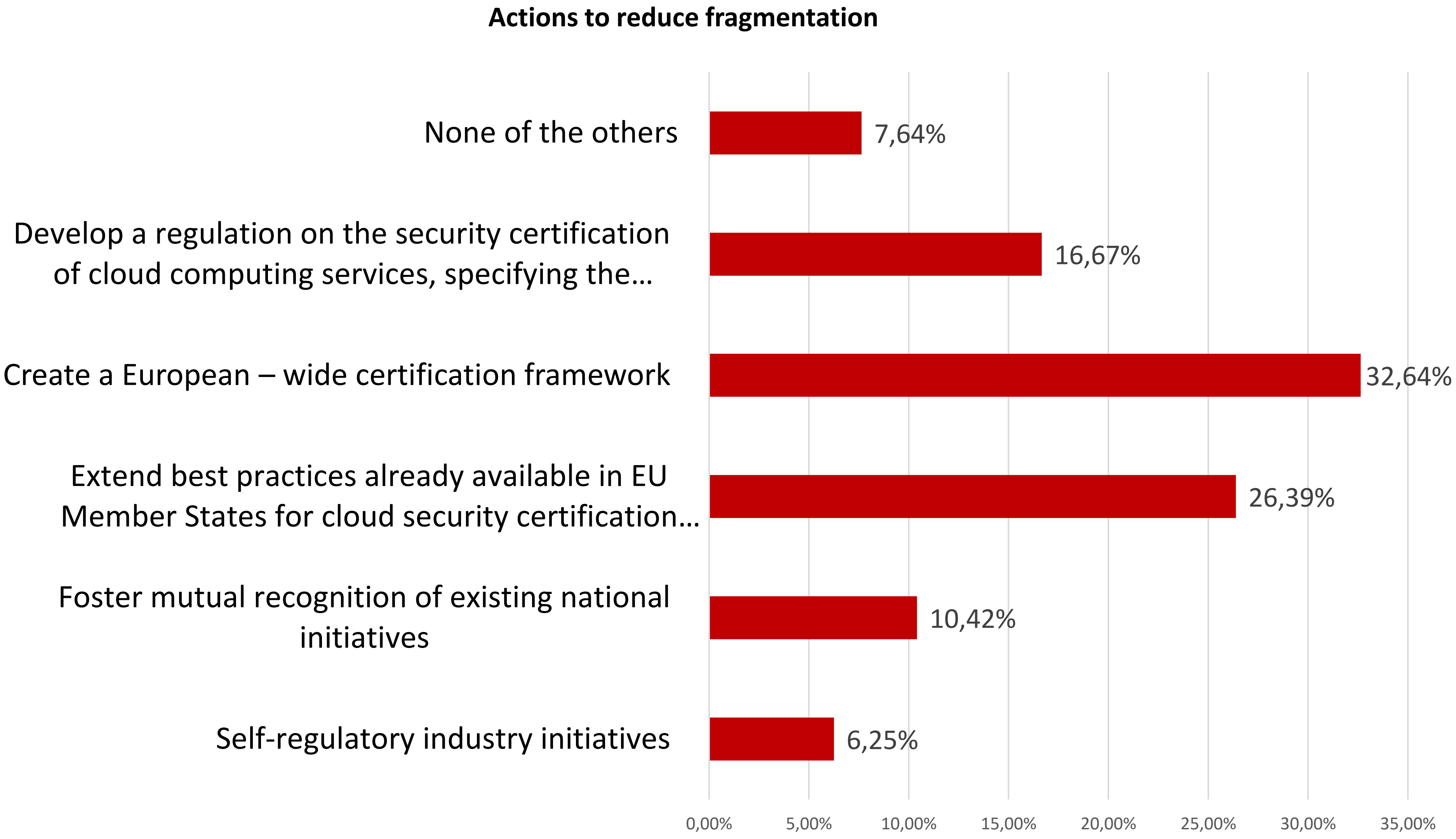
03 Stakeholders analysis



03 Stakeholders analysis Conclusions from the survey

- A certification scheme would increase the adoption of cloud computing (79,2% of the respondents)
- 56,94% believe that there should be one certification scheme per service layer
- 56,94% are aware of initiatives being ISO27001, C5, CSA Star, LEET security, Trusted Cloud, SecNumCloud the most named ones.
- 59% are aware of cross-border initiatives as well as good practices in cloud security
- 45% are aware of policy initiatives on cloud

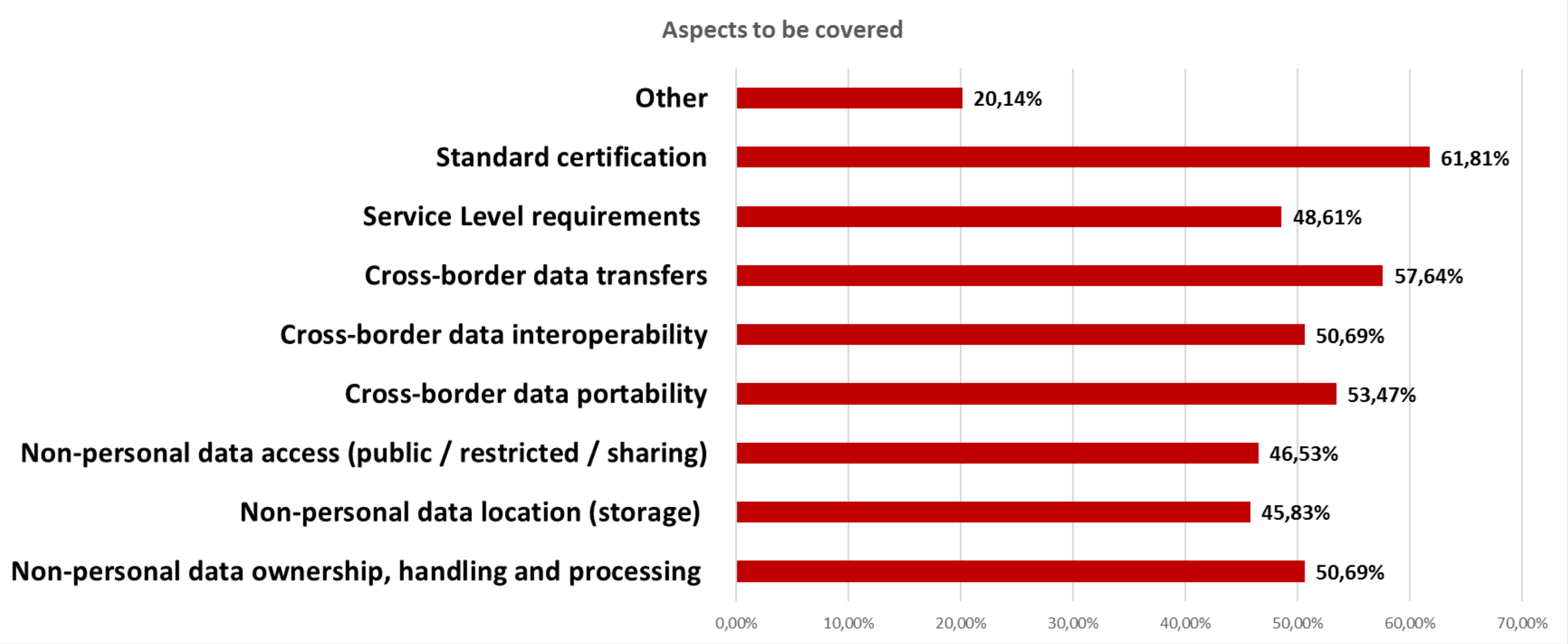
03 Stakeholders analysis Conclusions from the survey



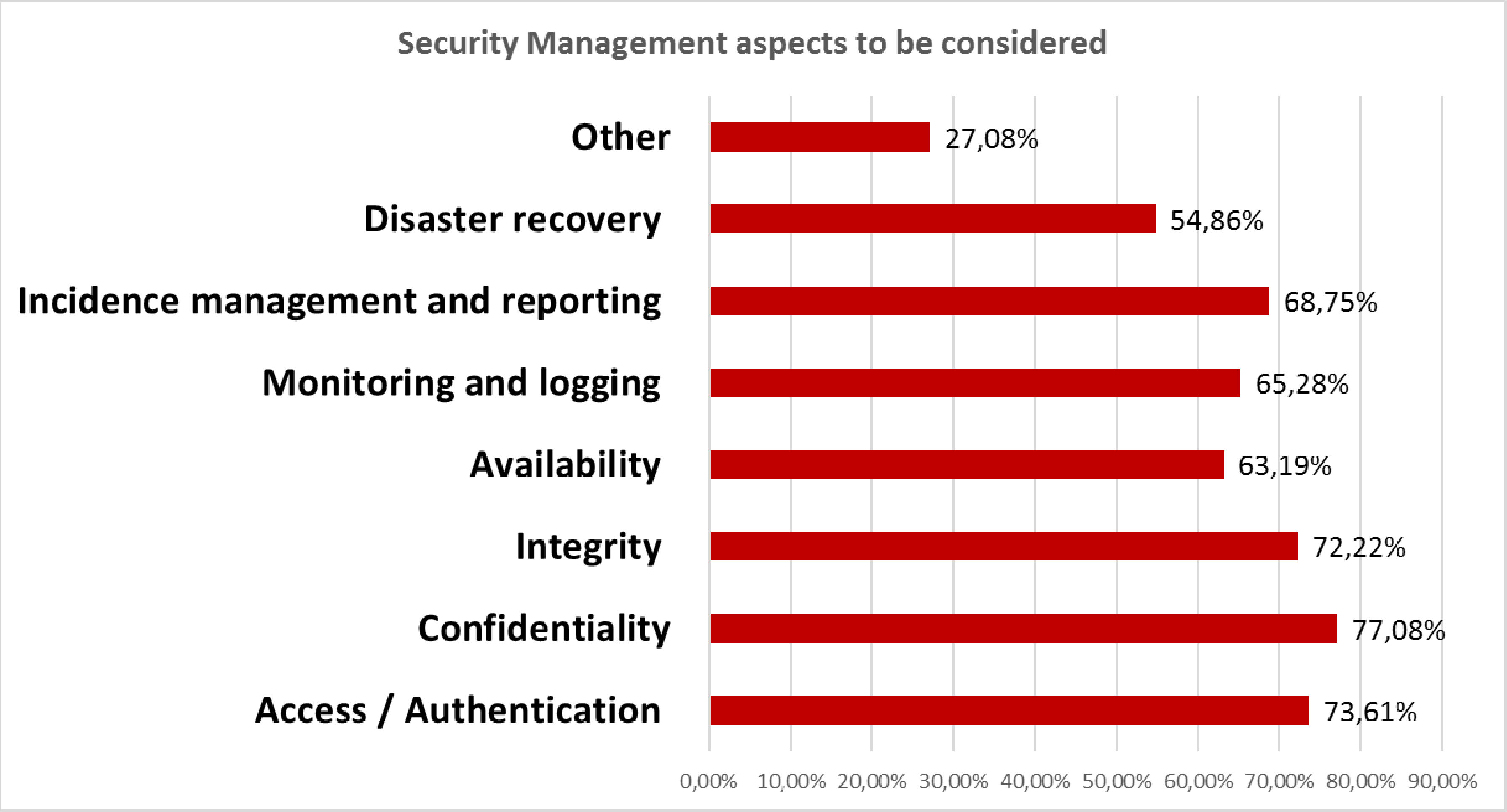
03 Stakeholders analysis Conclusions from the survey

- Provider of a certification scheme should be either an independent standardization body or an accredited institution (27.78% vs. 26.39%)
- Jurisdiction of the certification should be at EU-level

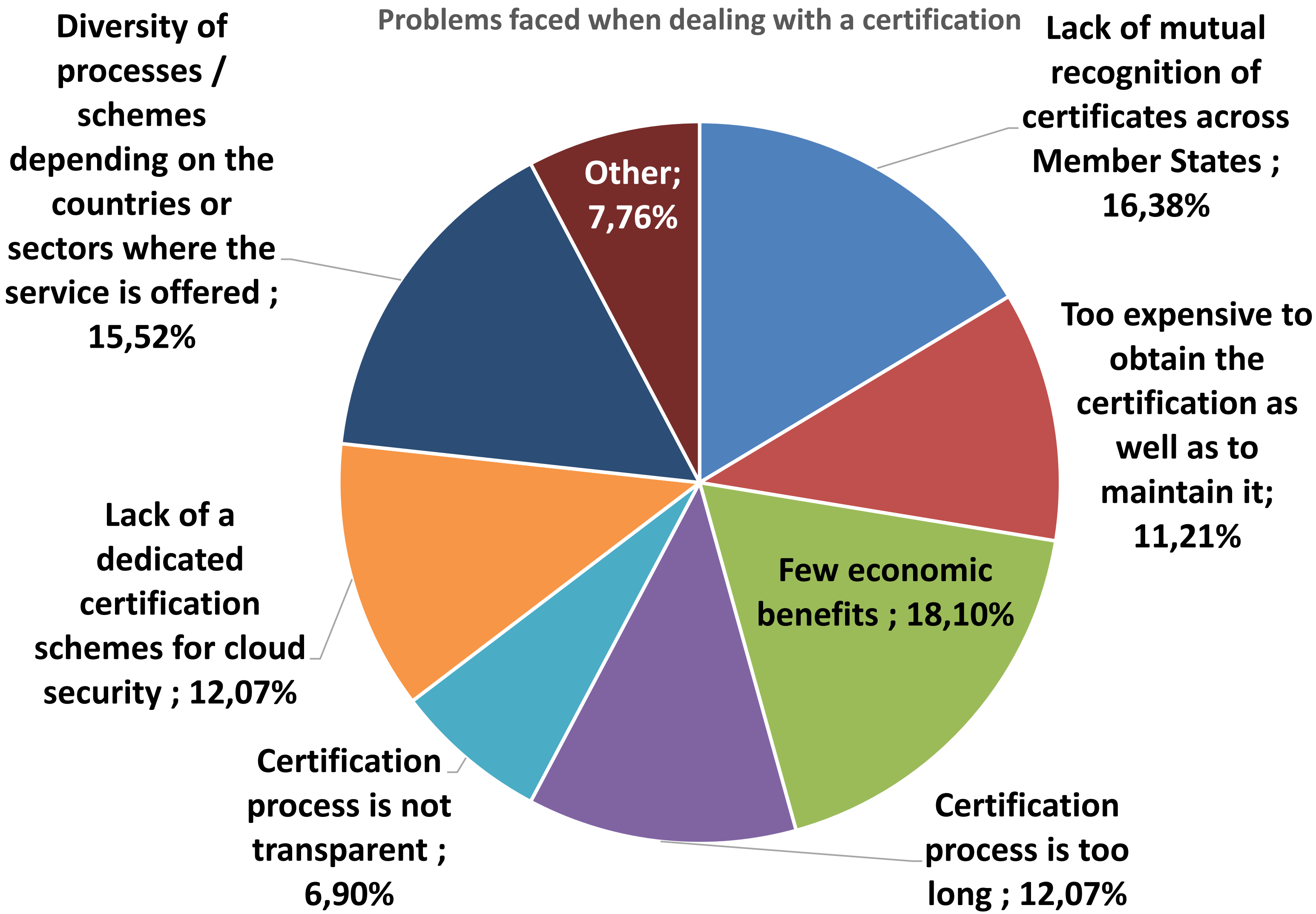
03 Stakeholders analysis Conclusions from the survey



03 Stakeholders analysis Conclusions from the survey



03 Stakeholders analysis Conclusions from the survey



03 Stakeholders analysis Conclusions from the survey

- Cost to obtain and maintain a certification is reported to be between 10,000 € – 100,000 €
- Recertification / renewal is mostly 1-3 years
- Certification is thought to prevent security incidents, which have occurred to 30% of the respondents with an economic impact of less than 100,000€, although most respondents have not quantified it
- Current fragmentation is a barrier to get a certification (65%)

03 Stakeholders analysis Conclusions from the survey

- The public sector and the EC should:
  - Lead and contribute to the definition of a security certification scheme, reusing and harmonizing existing initiatives
  - Set standards and applicable legislation
  - Be a Promoter and Influencer
- CSP Procurers of the public sector should be certified (92%)

Agenda

01 Context

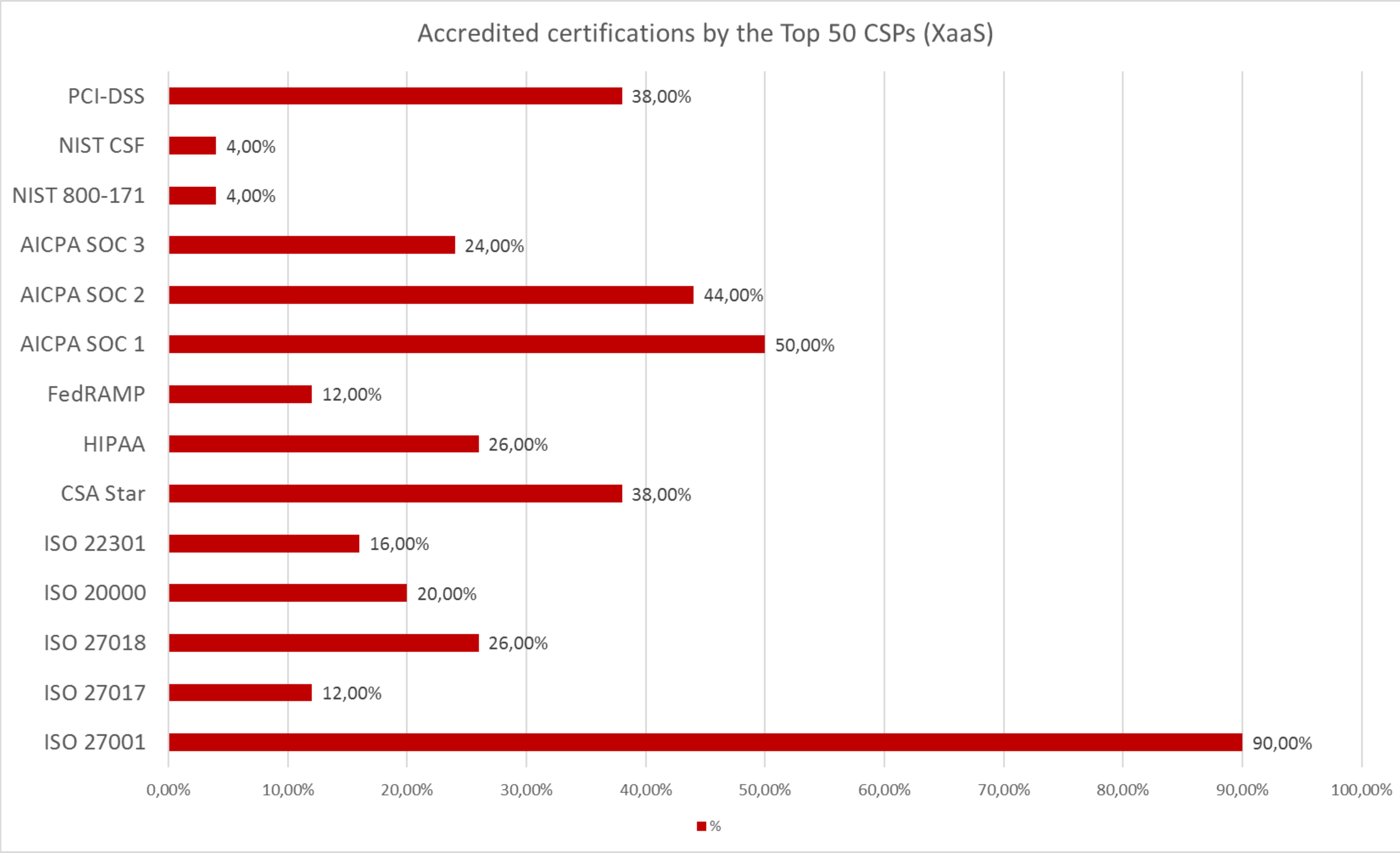
02 Approach

03 Stakeholders analysis

04 Market adoption

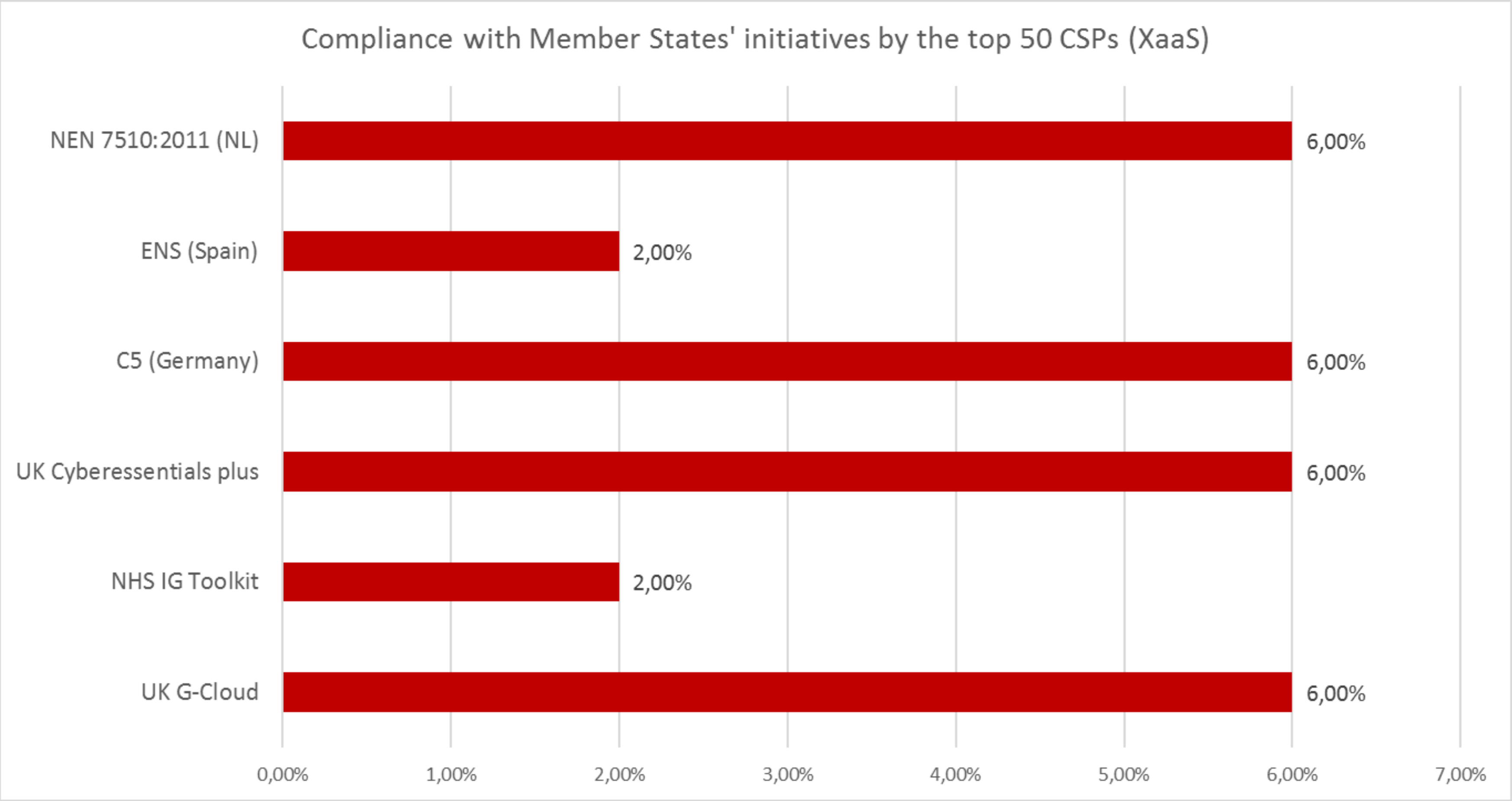
05 Next steps

04 Market adoption

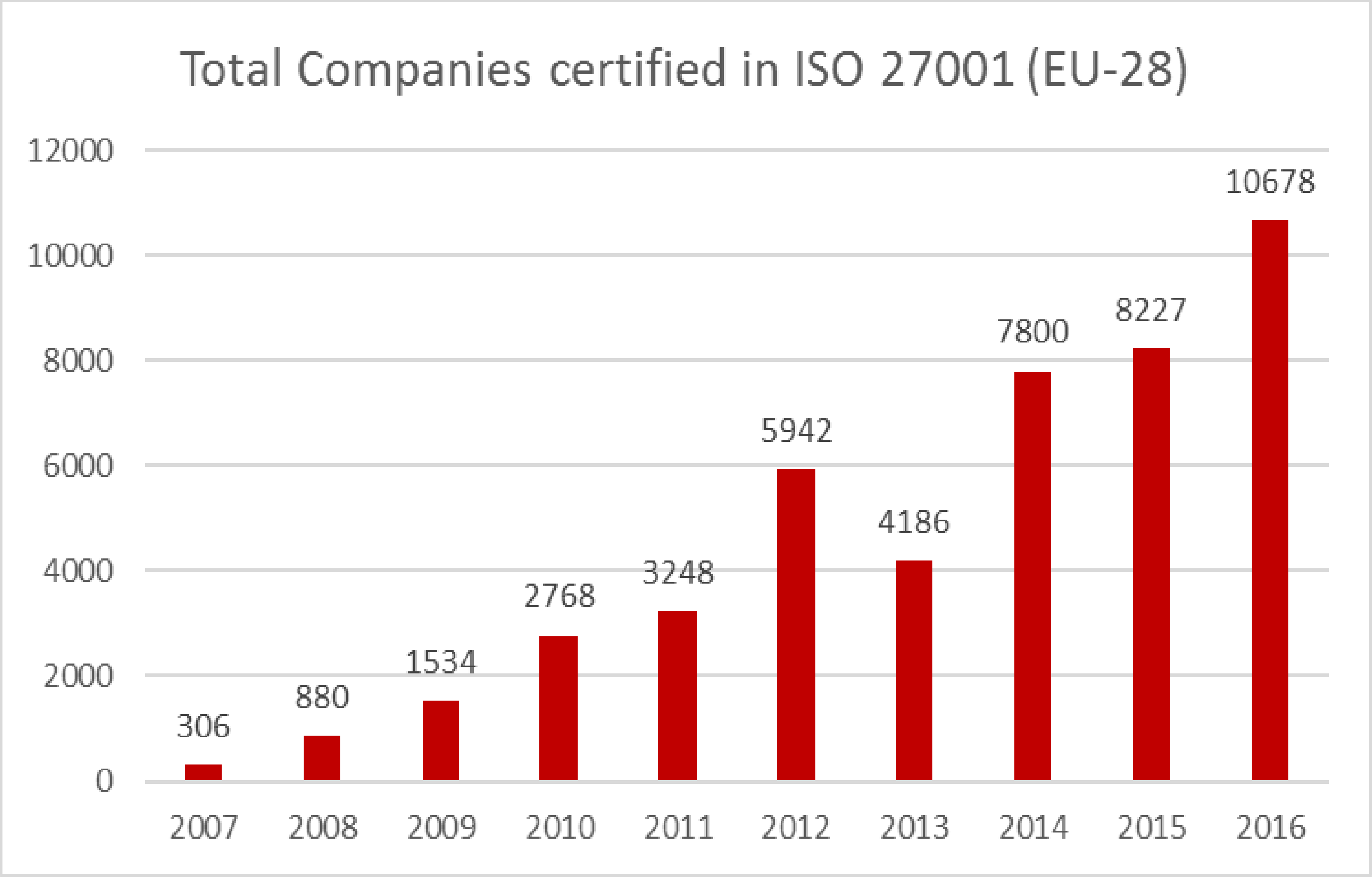


04 Market adoption

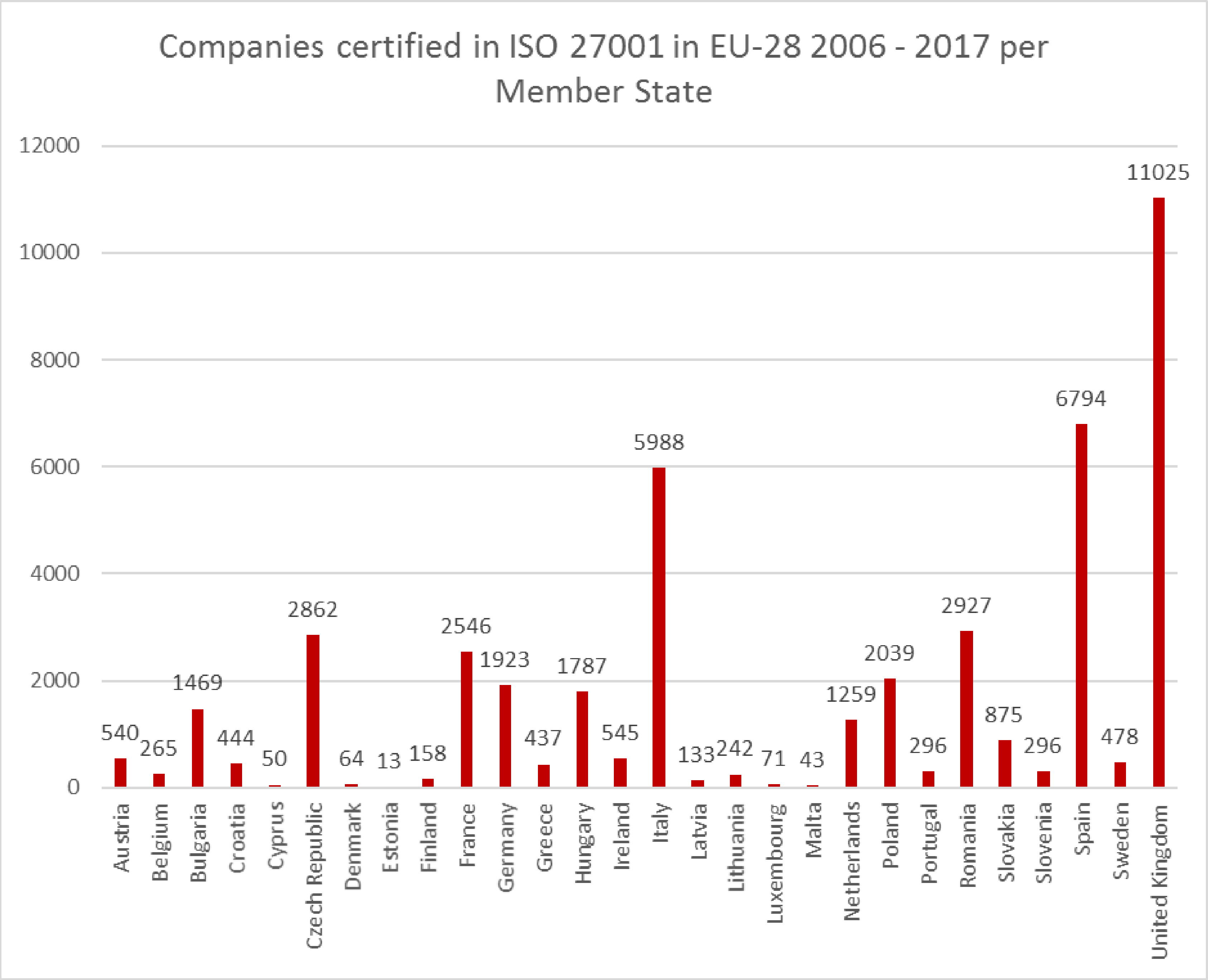
- Compliance with Member States’ requirements



04 Market adoption



(*) source: http://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1



Companies certified in ISO 27001 in EU-28 2006 - 2017 per Member State

(*) so

Agenda

01 Context

02 Approach

03 Stakeholders analysis

04 Market adoption

05 Next steps

05 Next steps

- In-depth analysis on the responses provided in the surveys
- Interview, if appropriate, more relevant actors
- Use these results, where appropriate, as input for the recommendations

Leire Orue-Echevarria Arrieta, MBA, PhD
División ICT / ICT Division
IT Competitiveness
Leire.Orue-Echevarria@tecnalia.com
C/ Geldo. Parque Tecnológico de Bizkaia, Edificio 700
E-48160 Derio - Bizkaia (Spain)
Tel: 902 760 000 *. Tel: +34 946 430 850 (International Calls).
Mob: +34 664 103 005

tecnalia Inspiring Business

Visita nuestro blog:
http://blogs.tecnalia.com/inspiring-blog/

www.tecnalia.com