WE
CAN DO
SO MUCH
TOGETHER

Challenges in the landscape of cloud security certification at EU level

Certification schemes for cloud computing

SMART 2016 / 0029

Maite Alvarez (TECNALIA)

Brussels, December 11th, 2017

tecnalia Inspiring Business

Agenda

01 Baseline

02 Scenarios

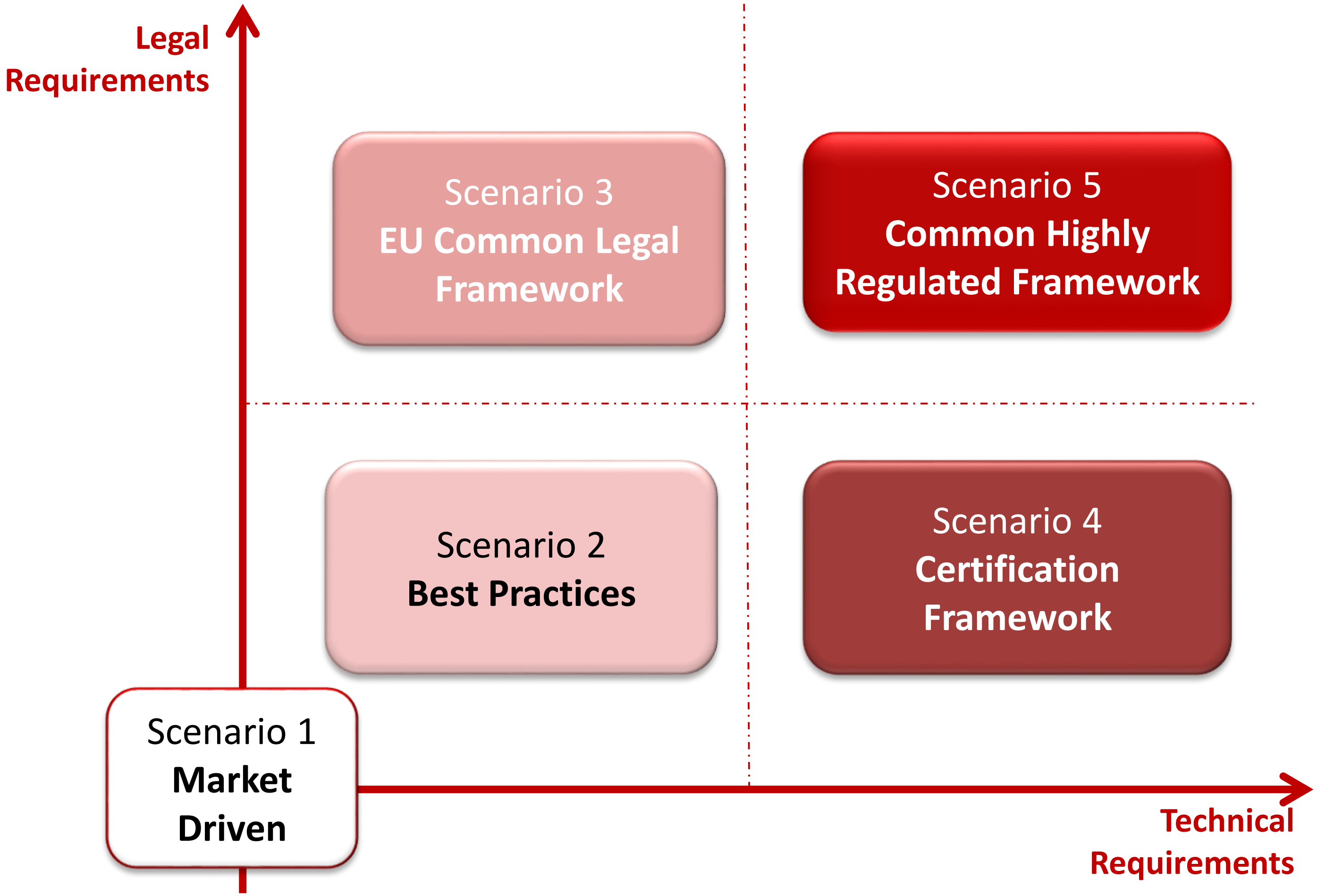
01 Common Baseline for Scenarios

- Two dimensions approach:
  - Legal requirements vs Technical requirements.

- Current situation:
  - Policy Framework in EU:
    - Digital Single Market Strategy (DSM)
    - General Data Protection Regulation (GDPR)
    - Free Flow of Data
    - NIS Directive
  - Technical vision
    - Multiple security standards, schemas and national initiatives.

01 Common Baseline for Scenarios

- Landscape of scenarios



Agenda

01 Baseline

02 Scenarios

02 Description of Scenarios

Scenario 1: Market driven

Description

No intervention from the Public Sector.
No additional EU common regulation (Member States decide).
Nor common certification framework, neither mutual recognition.

Contents

Current standard and regulation.

Example / Best Practice

"Let the market decide"

De facto standard can emerge, as VHS video format.

Pros

- Current infrastructure and instruments can be used.
- Consumers can identify easily that scheme as 'trustable'.

Cons

- Cannibalization of the market: ecosystem will be reduced to just a handful set of companies / certification institutions.
- Different legal jurisdictions (exception: personal data)

02 Description of Scenarios

Scenario 2: Best Practice

Description

Similar to *"Scenario 1: Market driven"*.
Desirable characteristics for providers and/or services are defined by the Public Administration in order to positively value different options in procurement processes.

Contents

Models for contracts and terms. Technical requirements to ask for (specially for critical services).
Evaluation criteria for suppliers and/or their products.

Example / Best Practice

"From best practice to standard"

ISO 27001 and ISO27002 standard coming from a best practice defined at national level initially defined by BSI (British Standard Institution).

Pros

- Reuse, 'not reinventing the wheel'
- Institutionalization of existing best practices is often easier
- Mutual recognition.

Cons

- Selection of a best practice as 'the one'

02 Description of Scenarios

Scenario 3: Best EU Common Legal Framework

Description

New set of EU regulation/directive defined for the whole EU. Default contract rules could be laid down for contractual terms between Public Administration (or any other business) and Cloud Service Providers

Contents

Non-personal data regulation.
Service Levels Agreements: security and other requirements.
Consumer protection or eGovernment regulation, etc.

Example / Best Practice

"Sharing legal requirements"

General Data Protection Regulation: a common regulation coming from a previous directive.

Pros

- Cloud-service consumers easily identify providers and services as 'trustable' as they need/require.
- Common legal jurisdiction (if regulation is defined).

Cons

- Complex solution, as many different points of views (technical, political …)
- Higher costs for cloud-service provider companies.

02 Description of Scenarios

Scenario 4: Certification Framework

Description

a) Mutual recognition
b) Promotion of a national initiative to a EU level
c) EU wide certification schema from scratch

Contents

Security certification schema/standard for CSPs.
a) Possible extension to regulation (EC) No 764/2008 (mutual recognition for goods).

Example / Best Practice

“Sharing Technical requirements”
a) Single market initiative, mutual recognition of education diplomas.
b) DINA4 as a EU standard.
c) Not known.

Pros

a) Broader market for CSPs. Cost effective solution for CSPs.
b) A starting point exists.
c) Focused on the interest of EU.

Cons

a) Unacceptance of quality service by customer not placed in the provider’s location.
b) The selection process is complex
c) Time, effort and resource consuming.

02 Description of Scenarios

Scenario 5: EU Highly Regulated Framework

Description

Highly ordered, policed and standardized situation.
Common legal framework for non-personal data applies at EU level. Additional obligations for critical cloud-services by law.
A common “EU CLOUD SERVICE LABEL” is outlined based on a meta-framework.

Contents

Same as Scenario 3 (Non-personal data regulation, SLAs, etc.)
Security Cloud-Service Standard Metaframework.

Example / Best Practice

“Energy Label”: An European Directive establishes a framework for labelling and standardization of consumer information regarding energy consumption for energy-related products.

Pros

- Common legal jurisdiction.
- Public can easily identify trustable Cloud Service Providers and/or services/products.

Cons

- Complex solution, as many different points of views (technical, political …)
- Higher costs for cloud-service provider companies.

Thank you!!

Maite Alvarez
División ICT / ICT Division
IT Competitiveness

maite.alvarez@tecnalia.com

tecnalia Inspiring Business

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

www.tecnalia.com