Dutch Authority for Digital Infrastructure
Ministry of Economic Affairs and Climate Policy

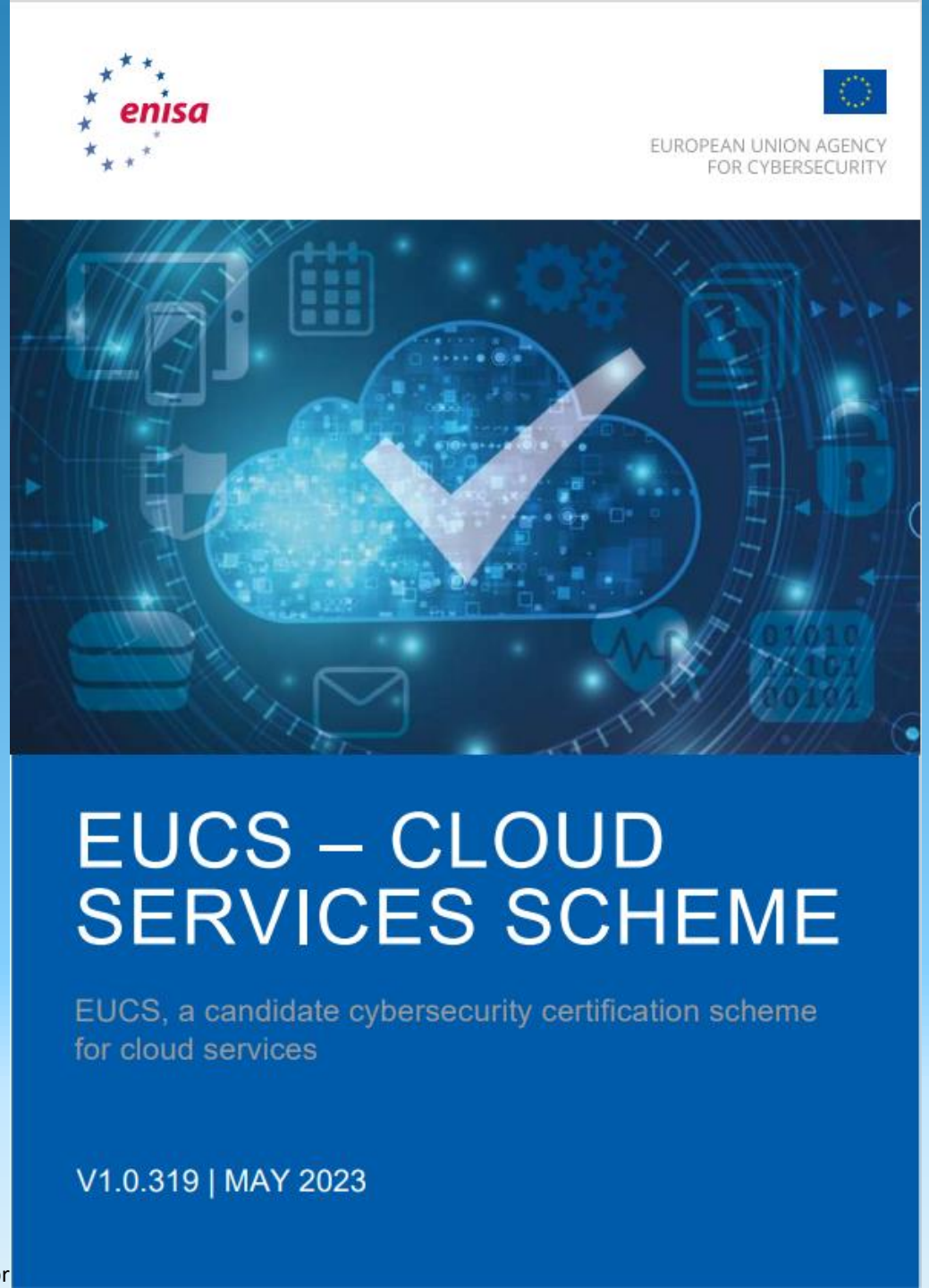
EUCS in depth

Stakeholdersmeeting 29 juni 2023

For a **safely connected** Netherlands

Speaker's name: Ruud Kerssens RE RA CISA CRISC

Date: 29 juni 2023

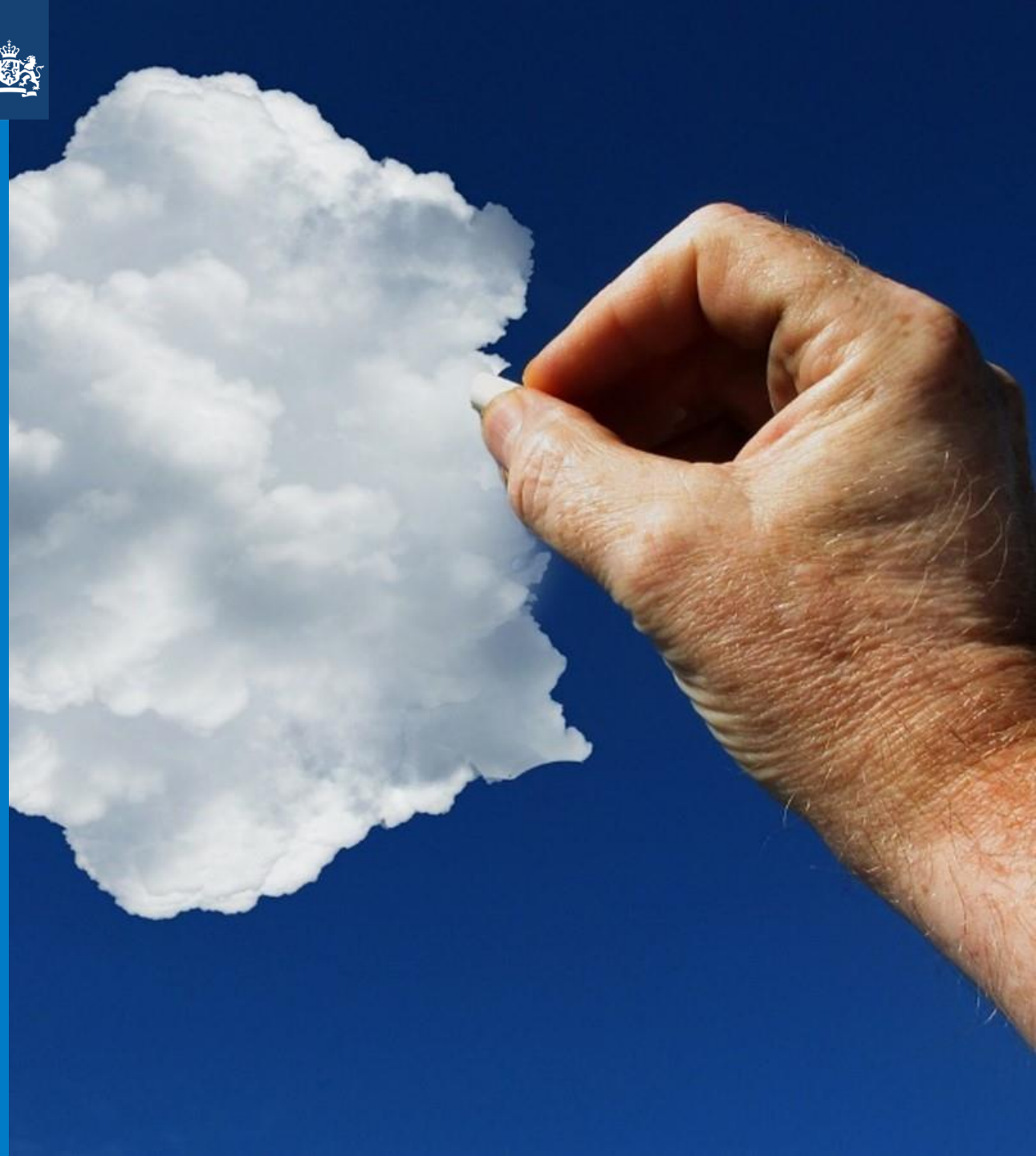


1. The current version of the scheme
2. CAB requirements
3. Conformity assessment meta-approach
4. Next steps

EUCS

The current version of the scheme

Version 1.0.319 05/05/2023 and shared per 15/5/2023

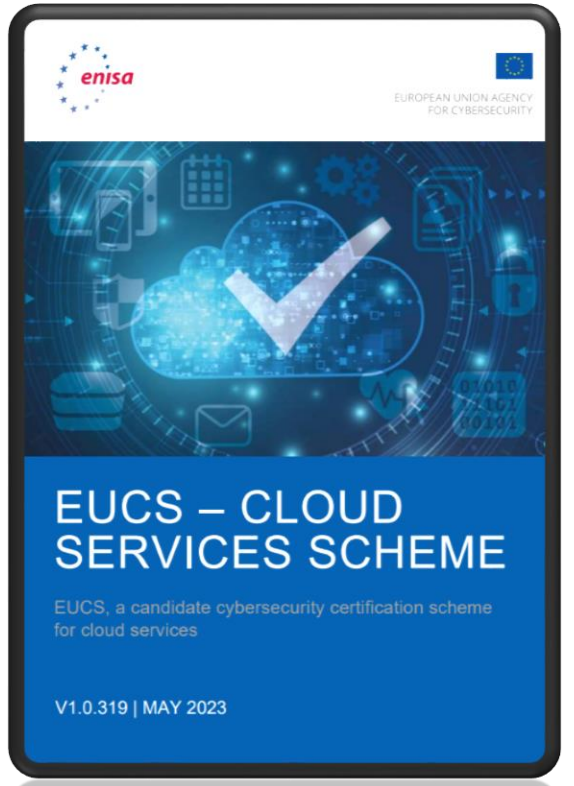


Current draft

- EUCS, a candidate cybersecurity certification scheme for cloud services
- a preparatory legal text .. for consultation under article 49 of the Cybersecurity Act (Regulation 2019/881)
- 334 pages
- 26 chapters
- Annex A → K

Key words introduction

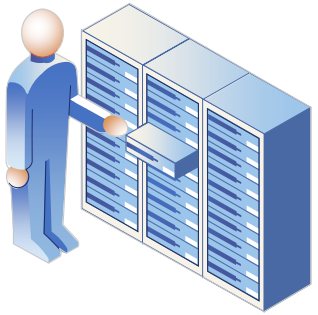
- Harmonized at EU level
- Third party assessment
- Supervision by national authorities
- “Assurance” levels Basic, Substantial and High
- Includes operating effectiveness guarantees
- Maintenance framework
- Integration European Cybersecurity Certification Framework
- “look at” EUCC



Some relevant aspects to know

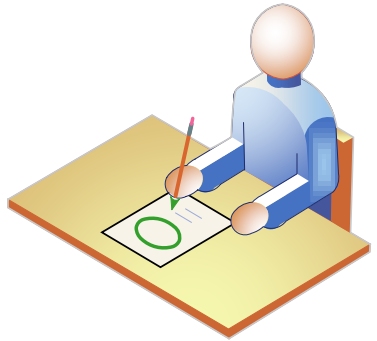
Purpose of the scheme

- improving the EU Internal Market conditions
- enhancing the level of cybersecurity of a wide range of cloud services



Cloud Service Provider

Cloud Service Customer



Regulatory Authority

Some relevant aspects to know

Subject matter and scope

- Required by art.54(1) CSA

*The ICT service implements one or more **cloud capabilities** offered via **cloud computing** invoked using a **defined interface***

One of the three levels 'basic', 'substantial' and 'high' of the CSA

- Acknowledgement responsibilities CSP and CSC
- prospects and customers with adequate cybersecurity knowledge for making informed security decisions on cloud services
- Focus is cybersecurity aspects, **not** compliance with other regulations

- Horizontal scheme, with the option of Extension Profiles CSEP
- Introduction of CS-EL = Evaluation levels
- to provide information to customers and allow them to make informed decisions
- Composition approach included in the scheme
- Relevance for other Regulation and schemes to be developed
- Role for Technical Specifications from CEN/CENELEC
- Expected additional requirements upon TS’s

Some relevant aspects to know

Assurance levels

Assurance Level	Requirements	Evaluation level	Level of expertise attacker	Available resources attacker	Evaluation activities	Outcome
Basic	Basic Security requirements including security functionalities.	Known basic risks of incidents and cyberattacks.			- Review of technical documentation; - ~~Option for self-assessment.~~	- ~~EU statement of conformity~~; - European cybersecurity certificate.
Substantial	Substantial Security requirements including security functionalities.	Known cybersecurity risks + risk of incidents and cyberattacks.	Limited skills.	Limited resources.	- Review to demonstrate the absence of publicly known vulnerabilities; - Testing to demonstrate compliance.	European cybersecurity certificate.
High	High Security requirements including security functionalities.	Risk of state-of- the-art cyberattacks.	Significant skills.	Significant resources.	- Review to demonstrate the absence of publicly known vulnerabilities; - Testing to demonstrate compliance state of the art; - Additional assessment of their resistance to skilled attackers, using penetration testing.	European cybersecurity certificate.

Example WD

10.7.OPS-07 Data Backup and Recovery – Monitoring

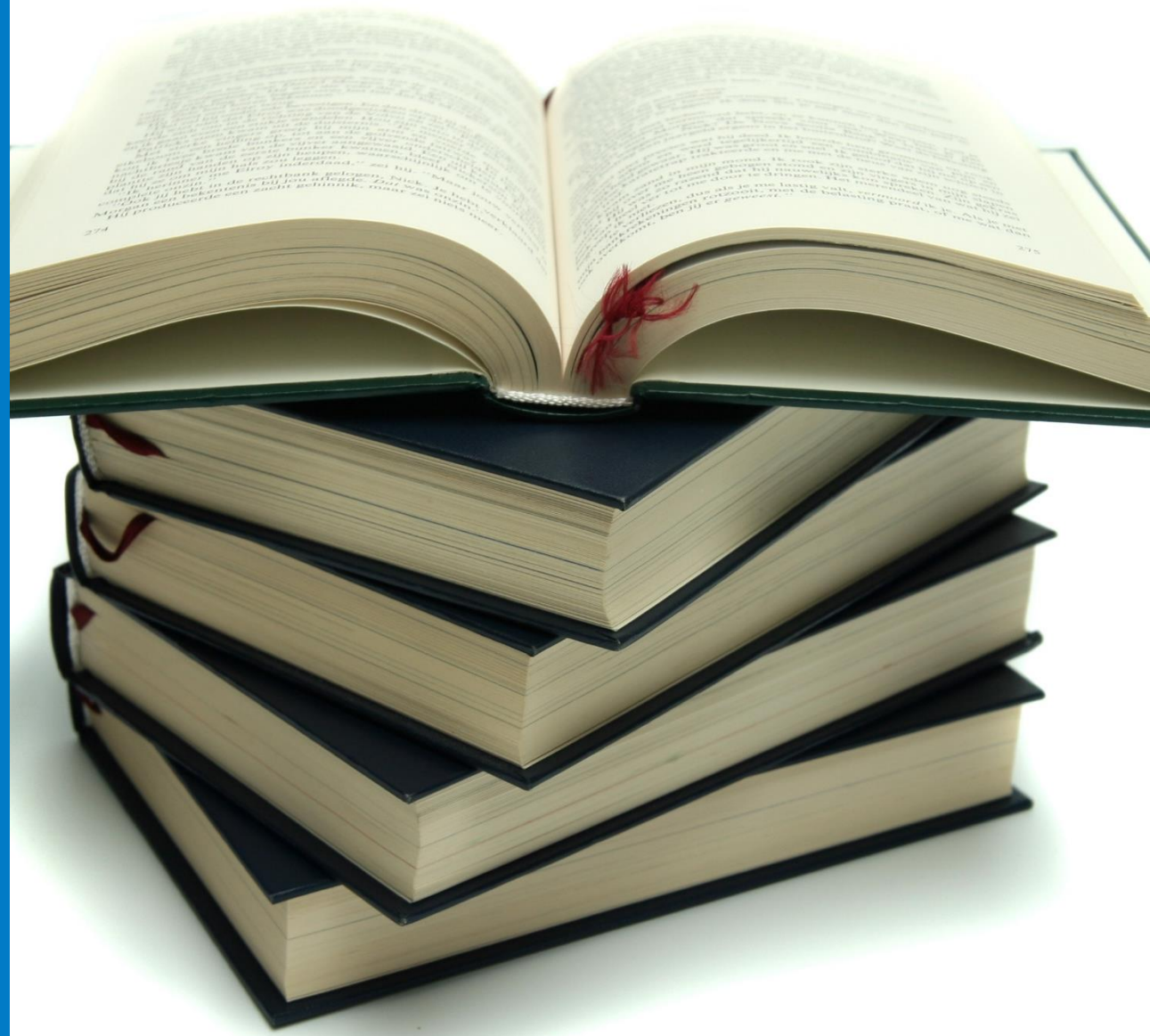
10.7.1. Objective

The proper execution of data backups is monitored.

10.7.2. Requirements

Basic	**The CSP shall document and implement technical and organisational measures to monitor the execution of data backups in accordance to the policies and procedures defined in OPS-06.**	OPS-07.1B
Substantial	The CSP shall document and implement technical and organisational measures to monitor the execution of data backups in accordance to the policies and procedures defined in OPS-06.	OPS-07.1S
High	The CSP shall document and implement technical and organisational measures to monitor the execution of data backups in accordance to the policies and procedures defined in OPS-06.	OPS-07.1H
	The CSP shall monitor the execution of data backups to check the implementation and consistency of these measures.	OPS-07.2H
	The CSP shall make information available to the CSCs for monitoring the execution of backups when the CSC uses backup services with the CSP.	OPS-07.3H

CAB Requirements



CAB requirements

General

- ISO 17065 accredited + Complemented EUCS requirements
- For HIGH including pentesting activities and competences
- *[at discussion]* ISO 17025 accredited for pentesting
- PUA criteria audit (legal / financial)
- Role in the Maintenance of EUCS

CAB requirements

Authorization

- CAB needs to be accredited
- Authorization request at NCCA (Assurance level High)
  - If additional requirements (now referred to as the Evaluation levels 3 and 4)
  - By the applicable NCCA
  - Including list of subcontractors (performing evaluation activities)
  - Stringent security requirements for protection of sensitive or protected information
- NCCA is required to assess (including the review of a pilot evaluation)

CAB requirements

Notification

- Notification request at NCCA to notify ENISA
  - Assurance level (highest applicable)
  - Including evaluation level
  - Listing subcontractors (including applicable evaluation level)

CAB requirements

Competencies …..

- CAB / Audit team / Role specific / Testing Lab
- Technical Specification CEN-CENELEC
- Cloud oriented (architecture and risk analysis)
- Case oriented
- Vulnerability identification
- Pentesting
- Development (source code…)
- System configuration and management

CAB requirements

Competencies .....

- Additional requirements from EUCS
  - Dependency analysis
  - Carve-out
  - Sampling ☺ and evaluation of results
  - Operating effectiveness
  - From PUA: legal and financial competencies

Conformity assessment meta approach

Structure

- EUCS
  - Annex B: Meta approach
  - Annex C: Assessment >= CS-EL 2
  - Annex D: Assessment CS-EL1
- Meta-approach

Meta-definition

- Audit → ISO 27000 / ISAE
- Assurance → Combined ISO/IEC 15408-1 and ISO/IEC/IEEE 15026-1
- Reasonable Assurance → ISAE 3000
- Limited Assurance → ISAE 3000

Meta method

Mapping controls to requirements (test once, rely often)

Regarding subservices:

- Inclusive

  Include the subservice provider in the audit scope

- Carve-out

  Exclude the subservice provider from the audit scope, but includes monitoring operating effectiveness

  CSOC’s (Complementary Subservice Organization Control) input Dependency analysis

- CUEC’s (Complementary User Entity Controls)

Assurance level in meta approach

- Assurance level
  - Basic = “limited assurance” for design and implementation
  - Substantial = “reasonable assurance” design, implementation and operating effectiveness
  - High = “reasonable assurance” design, implementation and operating effectiveness + resistance against attacks performed by skilled attackers
- Specified period
  - 6 months for evaluation level CS-EL2
  - 12 months for evaluation levels CS-EL3 and CS-EL4

Evaluation levels

Assurance level	Evaluation level
Basic	CS-EL1
Substantial	CS-EL2
High	CS-EL3
High	CS-EL4

PUA	Name	Doelstelling
PUA-01	Primacy of EU law	The CSP operates primarily within the legal framework provided by the EU and its Member States, with precedence over laws from non-EU states that may include extra-territorial measures.
PUA-02	Operation in the EU	The cloud service is operated and maintained from the EU, and all CSC data is stored and processed in the EU.
PUA-03	Controlling exchanges with employees and suppliers outside of the EU	The exchanges between the cloud service and its employees and suppliers are controlled specifically when the employee or supplier is located outside of the EU.
PUA-04	Control requirements	Certified cloud services are operated only by companies based in the EU, with no entity from outside the EU having effective control over the CSP, to mitigate the risk of non-EU interfering powers undermining EU regulations, norms and values.

Next steps

Not to be predicted

- Comments from ECCG to be discussed
- Version for consultation
- Draft Implementing Act
- Etc.

Live:

- One year for Authorization / Notification
- Certification starting after that year
- Ceasing existing schemes

Dutch NCCA

- Updates EUCS specific
- In depth sessions / workshops
- Identifying and contacting interested CAB’s
- Information for CSP’s
- Etc.

Any questions?