Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

EUCS, EU rol en impact

Voor een **veilig verbonden** Nederland

Ruud Kerssens RE RA CISA CRISC

OTC Webinar, 17 februari 2022

ONLINE TRUST COALITIE

EUCS – CLOUD SERVICES SCHEME

EUCS, a candidate cybersecurity certification scheme for cloud services

1. Het fundament voor het EUCS
2. De rol van het EUCS
3. Het EUCS
4. Impact voor dienstenleveranciers en gebruikers

Het fundament voor het EUCS

- Certificeren op basis van het EU Cloud Services scheme

Waarom?

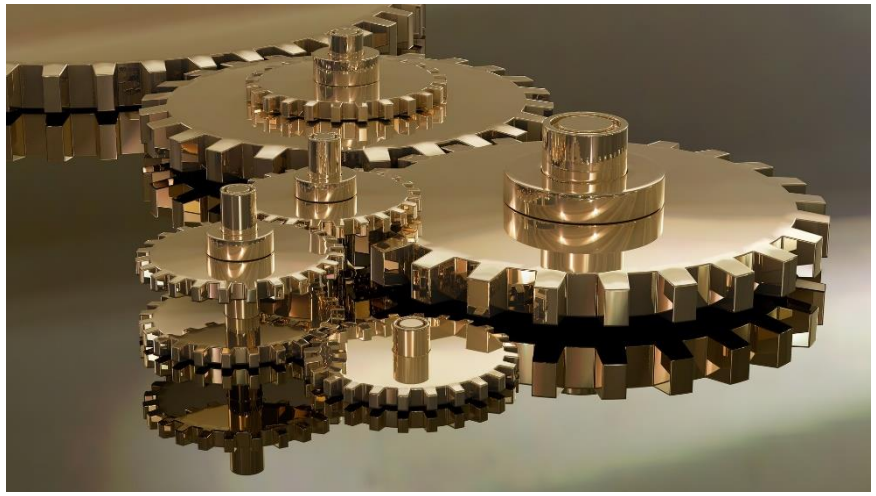
- Cybersecurity Act [2019/881]:
  - Afhankelijkheid van ICT
  - Toenemende cyberrisico's
  - Cyberbeveiligingskenmerken onbekend
  - Grensoverschrijdend vergt EU actie
  - Verhogen cyberweerbaarheid
  - Vertrouwen verdienen

  = **Uniebrede certificering** op basis van gemeenschappelijke cyberbeveiligingsvoorschriften en evaluatiecriteria (schema's)

- Schema's?
  - URWP (Union Rolling Work Program)
  - Verzoek European Commission

  Waarom dan EUCS?
  - EUCC voor producten (bestaande Common Criteria certificatie)
  - EUCS in het URWP genoemd als eerste prio na EUCC voor "Future candidate scheme"
  - Opdracht aan ENISA (december 2019)
  - Cloud veel gebruikt + de basis voor innovatieve diensten (AI, big data, blockchain)

Belangrijkste elementen CSA



- Trustworthiness **Conformity**
- Certification schemes: non-discriminatory + gebaseerd op Europese of internationale standaarden
- Security Objectives
- Requirements (availability, authenticity, integrity, confidentiality)
- Geldig binnen heel de EU = **harmonisatie**
- **Uitfaseren** bestaande nationale schemes = harmonisatie

- ICT producten, processen en diensten
- (Evaluatie) **Assurance levels**: Basic, Substantial and High
- *"Implemented* and *supervised* by NCCA's"
- Vrijwillig, maar ….

De rol van het EUCS

NB: informatie over aangehaalde wetgeving AI en NIS2:
Dit zijn versies die in onderhandeling zijn. De informatie is gebaseerd op de laatste, publiek beschikbare, conceptversies. Dit betekent dat zij nog onderhevig zijn aan wijzigingen. Die ook nog substantieel kunnen zijn.

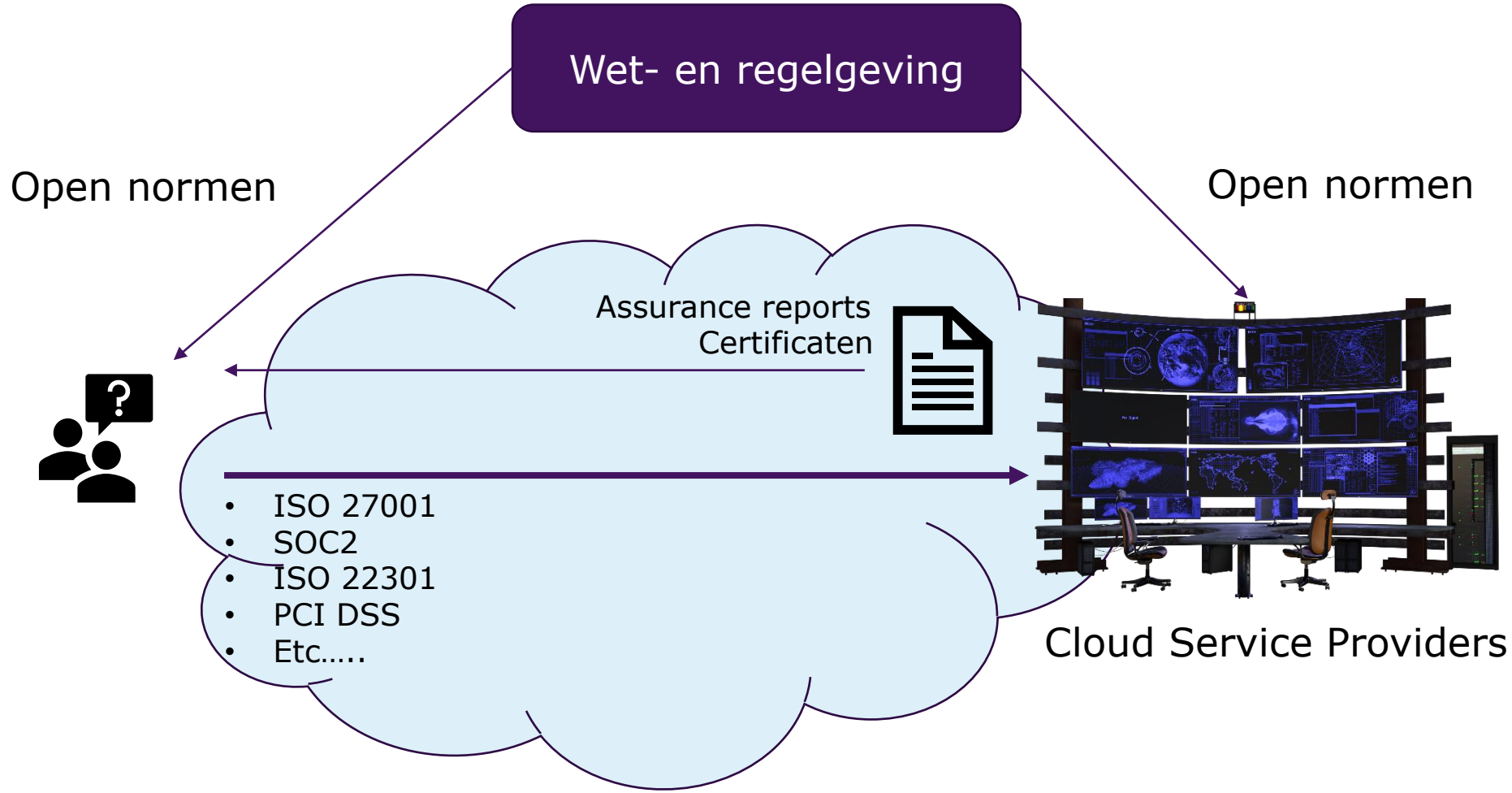
Vrijwillig?

Voluntary

- *should remain voluntary*
- ***unless*** *otherwise provided for* ***in Union law***
- *or* ***in Member State law*** *adopted in accordance with Union law in absence of harmonized Union law … [Directive (EU) 2015/1535]*
- ***in the context of public procurement*** *[Directive 2014/24/EU]*

Dus mogelijkheid verplicht te stellen

Normen en standaarden



speelveld

Wet- en regelgeving

EU Wet- en regelgeving

CSA

Certificatie Schema's

Open normen

Open normen

Gesloten normen

Assurance reports
Certificaten

- ISO 27001
- SOC2
- ISO 22301
- PCI DSS
- Etc…..

Cloud Service Providers

Vrijwillig?

AI Act (draft)

Artikel 42: Presumption of conformity with certain requirements

- artikel 10 - data and data governance +
- artikel 15 - Accuracy, robustness and cybersecurity
  - *"High-risk AI systems that have been certified …"*
  - *"shall be presumed to be in compliance with the cybersecurity requirements …"*
  - *… "in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements."*

Maar: Nog heel veel andere gedetailleerde eisen! Die niet gekoppeld aan de CSA.

Vrijwillig?

NIS 2 (draft) = Directive

Article 21 - Use of European cybersecurity certification schemes

- [1] "In order to demonstrate compliance with certain requirements.."
- **Member States** may **require** entities to use particular ICT products, ICT **services** and ICT processes **certified** under specific **European cybersecurity certification schemes**….
- [2]"**The Commission** may adopt implementing acts specifying which categories …."
- shall be **required** to … obtain a certificate and under which specific **European cybersecurity certification schemes**

Daarnaast nog steeds specifieke vereisten zoals rapporteren over cyber incidenten, risicomanagement.

Scope

Essential entities

– Energy (electricity—now including **production**; **aggregation**; **demand response** and **energy storage**; **electricity markets**—; **district heating**; oil; gas and **hydrogen**)
– Transport (air; rail; water; road)
– Banking
– Financial market infrastructures
– Health (healthcare; **EU reference labs**; **research and manufacturing of pharmaceuticals and medical devices**)
– Drinking water
– **Waste water**
– Digital infrastructure (IXP; DNS; TLD; cloud; **data centre service providers**; **CDN**; **trust service providers**; **electronic communications**)
– **Public administrations**
– **Space**

Important entities

– **Postal and courier services**
– **Waste management**
– **Chemicals (manufacture; production; distribution)**
– **Food (production; processing; distribution)**
– **Manufacturing (medical devices; computer, electronic and optical products; electrical equipment; machinery; motor vehicles and (semi-)trailers; transport equipment)**
– Digital providers (online marketplaces; search engines; **social networks**)

Het EUCS

EUCS – CLOUD SERVICES SCHEME

EUCS, a candidate cybersecurity certification scheme for cloud services

DECEMBER 2020

Het schema

- *Doel*
- *Scope*
- *Definities*
- *Standaarden*
- *Assurance levels*
- *Eisen aan conformity assessment bodies*
- *Evaluatie methoden*
- *Labelling*
- *Certificaat management*
- *Non-compliance*
- *Nieuwe kwetsbaarheden*
- *Geldigheid certificaten*
- *A: Security objectives and requirements*
- *B: Meta approach for the assessment*
- *H: Extension profiles (CSEP)*

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; - Additional assessment of their resistance to skilled attackers, using penetration testing.	European cybersecurity certificate.

Voorbeeld

- “shall” = vereiste;
- “should” = aanbevolen;
- “may” = zou kunnen;

5.4 HR-04 SECURITY AWARENESS AND TRAINING

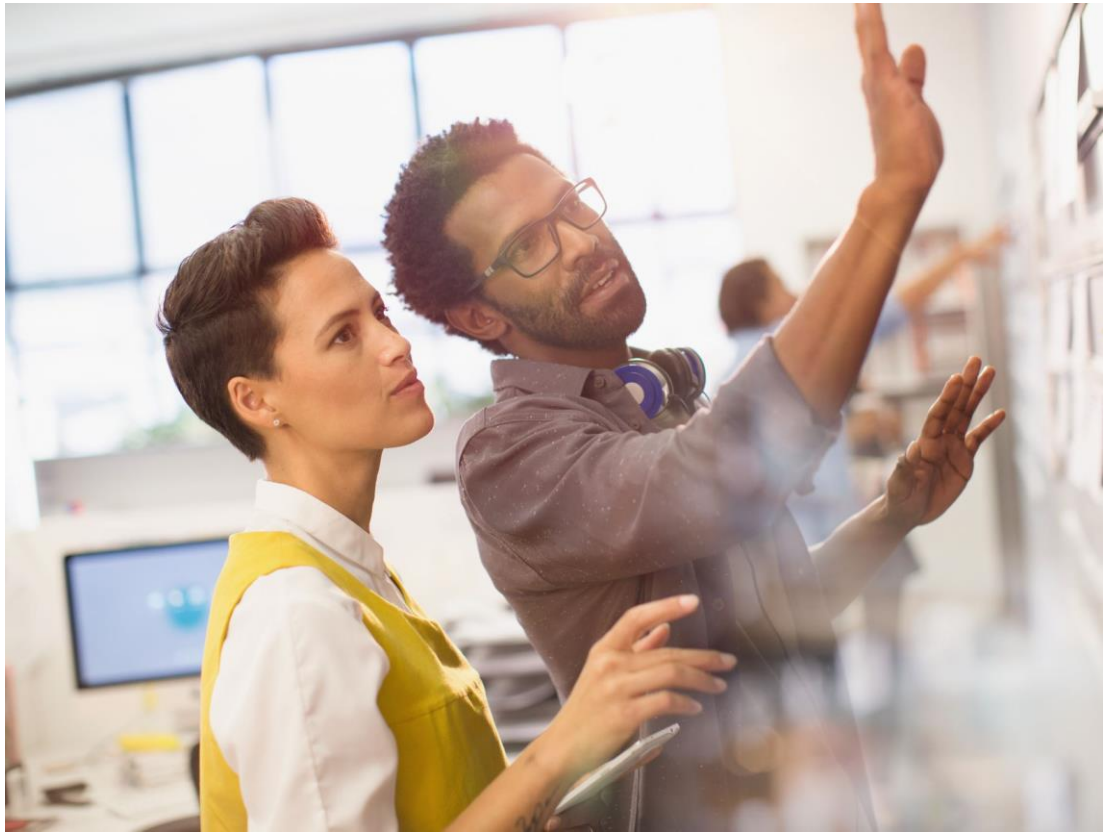
5.4.1 Objective

The CSP operates a target group-oriented security awareness and training program, which is completed by all internal and external employees of the CSP on a regular basis.

5.4.2 Requirements

Basic	**The CSP shall define a security awareness and training program that covers the following aspects:** • **Handling system components used to provide the cloud service in the production environment in accordance with applicable policies and procedures;** • **Handling cloud customer data in accordance with applicable policies and instructions and applicable legal and regulatory requirements;** • **Information about the current threat situation; and** • **Correct behaviour in the event of security incidents.**	HR-04.1B
	The CSP shall review their security awareness and training program based on changes to policies and instructions and the current threat situation.	HR-04.2B
	The CSP shall ensure that all employees complete the security awareness and training program defined for them.	HR-04.3B

Assessment (Substantial / High)



- ISO 17065:2012 + ISAE = hoe de assessment te doen
- + werking en redelijke mate van zekerheid!
- Assertion based : CSP stelt de beschrijving op en bevestigt deze;
- Subservices zijn in scope (opties “inclusive”, “carve-out”) (bij carve out **ook gebruik Assurance rapporten (subservice) organisatie**);
- Complementary controls (CCC’s en CSOC’s ☺)
- Mapping eigen “controls” met Security requirements;
- kan (maar dan wel “complete, accurate and valid”) (aandachtspunt, vooral bij ketenproblematiek);
- EUCS = “mandatory baseline”.

Extra bij HIGH

- Dus meer en zwaardere “Security requirements”
- Aangetoonde weerbaarheid tegen aanvallen van ervaren aanvallers → test door ISO 17025 geaccrediteerd laboratory EN geautoriseerd door de NCCA

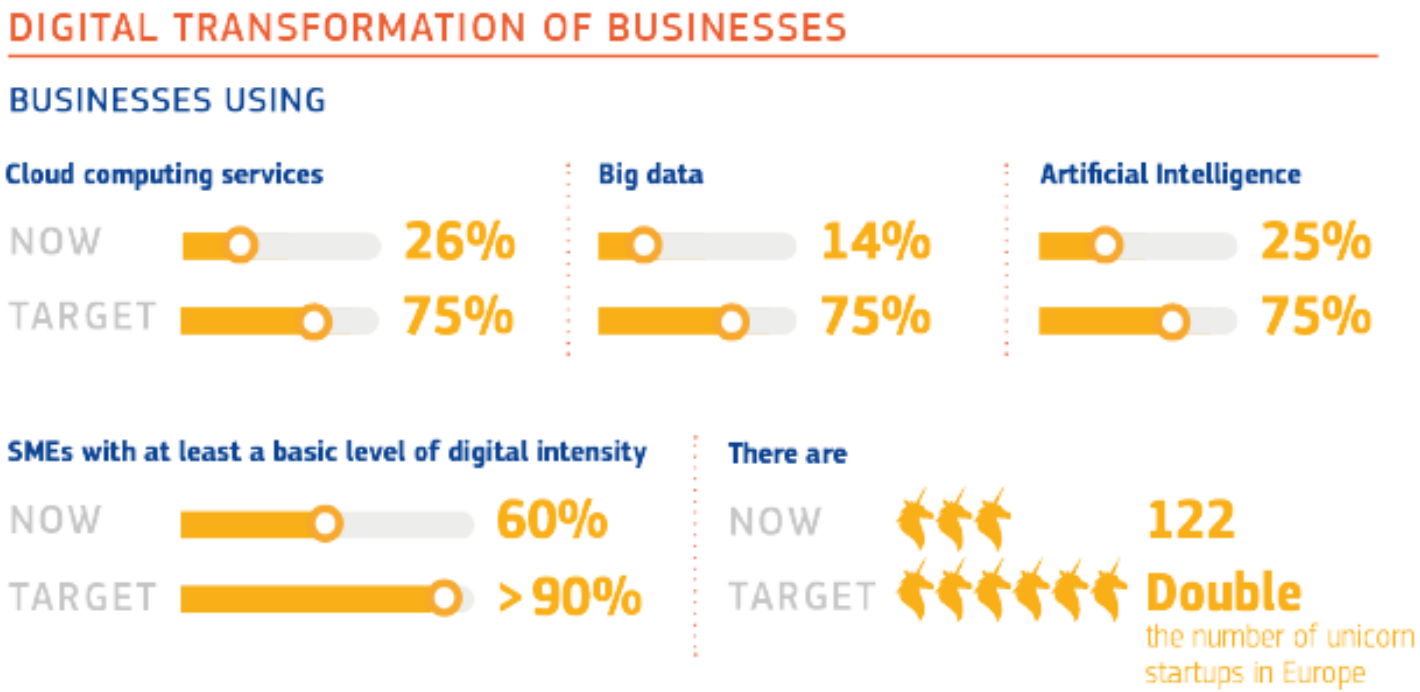
Impact voor gebruikers en Cloud diensten-leveranciers

EUCS – CLOUD SERVICES SCHEME

EUCS, a candidate cybersecurity certification scheme for cloud services

DECEMBER 2020

EC Policy program voor 2030



Samengevat

Gebruiker	Cloud dienstenleverancier
• Nieuwe regelgeving verwijst naar certificatie.	• Nieuwe regelgeving verwijst naar certificatie.
• Die is nog in ontwikkeling en niet definitief = onzekerheid.	• Die is nog in ontwikkeling en niet definitief.
• Steeds meer organisaties en gebruikers in scope.	• Certificatie-eis: via gebruikers en rechtstreeks (bv. NIS2).
• Inzicht in de keten en afspraken met ketenpartners nodig.	• Tendeert naar vereist niveau HIGH voor Cloud Service leveranciers.
• Ook specifieke eisen, aanvullend in wet- en regelgeving.	• Gedetailleerde vereisten in de schema's.
• Monitoring controls op cloud service leverancier noodzakelijk.	• Inzicht in sub services van groot belang i.c.m. rol risicoanalyses.
• Ook Complementary controls in te vullen.	• Aanpassingen in de Cloud architectuur noodzakelijk.
• Hogere kosten voor gebruik cloud services / sub services in Europa.	• Hogere auditkosten, Assurance rapporten verlichten de auditlast.

Dus “Change of play” op EU niveau

- Certificering belangrijke maatregel regelgever, hulpmiddel Cloud service organisatie en bewijsstuk gebruiker;
- Je bent snel in scope en voor de HIGH criteria;
- **Bereid je voor**:
  - Analyse gebruikers en impact wet- en regelgeving (ben ik in scope en voor wat?) en bepaal gewenst Assurance level;
  - Afhankelijkheidsanalyse sub services / Cloud services;
  - Nulmeting;
  - Projectmatig realiseren van tekortkomingen;
  - Betrekken Assurance auditor (let op afspraken gebruikerskring en inhoud Assurance rapport);
  - Op zoek naar een Conformity Assessment Body.

Voor een **veilig verbonden** Nederland

www.agentschaptelecom.nl

info@agentschaptelecom.nl

communicatie@agentschaptelecom.nl