EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBERSECURITY CERTIFICATION OF CLOUD SERVICES *STANDARDS? WHICH STANDARDS?*

Eric Vetillard, Ph.D.
Lead Certification Expert, MCS, ENISA
Char, EUCS AHWG

07 | 02 | 2023

FROM THE CYBERSECURITY ACT

Standardisation is at the heart of the definition of European cybersecurity certification schemes

In recitals

- (53) ENISA should regularly consult **standardisation** organisations, in particular European **standardisation** organisations, when preparing the European cybersecurity certification schemes.
- (69) The European cybersecurity certification schemes should be non-discriminatory and based on European or international **standards**, unless those **standards** are ineffective or inappropriate …

And in Article 54, which defines the elements of a scheme

- (b) a clear description of the purpose of the scheme, and how the selected **standards**, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme;
- (c) references to the international, European or national **standards** applied in the evaluation or, where such **standards** are not available or appropriate, to **technical specifications** …

EUROPEAN CLOUD SERVICES SCHEME (EUCS): A GENERIC SCHEME

All capabilities

Also based on ISO/IEC 22123-1

All cloud capabilities are supported: Infrastructure, Platform, Application

Covers the full stack

No mention of deployment model

Horizontal

Defines a baseline of requirements that are applicable to all services.

Enables the same methodology for all services

Does not assess the security of product-specific security features (Security as a Service)

3 evaluation levels

Mapped to assurance levels as defined in the European Cybersecurity Act

‘basic’

‘substantial’

‘high’

All levels based on an assessment by an accredited third-party

REQUIREMENTS FOR CLOUD SERVICES

We haven't found a matching standard, so we designed our own requirements and later submitted them to CEN-CENELEC JTC13 WG2.

The EUCS has quite specific issues

- The object of certification is a cloud service, not a management system
- We have a requirement to address multiple assurance levels and therefore multiple sets of requirements
- We have to be compliant with the Cybersecurity Act, which has a few "exotic" requirements

Work is ongoing in WG2, with a few interesting debates

- Overall, it led to many improvements of the requirements
- Positioning with respect to ISO/IEC 27001 has been/is the most difficult issue to tackle

REQUIREMENTS FOR EUCS CABS

These requirements are based on ISO/IEC 17065 but they include some methodology components that are specific to the EUCS.

Once again, the EUCS has specific issues

- There are several assurance levels, including a ‘basic’ one that has lower expectations than usual schemes
- This is a full-stack audit, so some assurance information is required from subservice providers
- The scheme decided early on that the evaluation activities should be shareable with other assessment activities
  - In particular, we are thinking of ISO/IEC 27001 certification and of reporting following ISAE standards (*e.g.*, C5, SOC2)

We also had some interesting exchanges in CEN-CENELEC JTC13 WG3 around this

- Questioning the status quo is sometimes difficult, but in our case required by the Cybersecurity Act
- Making different communities exchange remains difficult, but easier in the EUCS AHWG

OTHER ISSUES

We have a few more issues to address, which are not currently in discussion with SDOs, but could be candidates.

Vulnerability assessment activities, including pen testing

- The scheme requirements mandate at the highest level the use of an external party
- The scheme itself says that this external party shall be accredited and authorized (*i.e.*, a CAB)
- Some requirements for this activity will be drafted this year
- Traditionally based on ISO/IEC 17025, but in fact, looks closer to ISO/IEC 17020…

Sovereignty issues, anyone?

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Ethnikis Antistaseos 72 & Agamemnonos 14, Chalandri 15231
Attiki, Greece

+30 28 14 40 9711

certification@enisa.europa.eu

www.enisa.europa.eu