NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

ENISA

Datum : 14 september 2023
Kenmerk : NOREA/AB-wo23-138
Betreft : **Evaluation ENISA and the EU Cybersecurity Certification Framework**

Introduction and summary

This is the response of NOREA, the professional association of IT auditors in the Netherlands, to the European Commission's (DG CNECT) call for evidence for an evaluation / fitness check of ENISA (European Union Agency for Cybersecurity) and the Cybersecurity framework. The current mandate of ENISA is to contribute to achieving a "high common level of cybersecurity across the Union", "act as a reference point for advice and expertise on cybersecurity" and "contribute to reducing the fragmentation of the internal market". For these goals ENISA performs a number of tasks. This response focusses on ENISA's efforts to create a cybersecurity certification scheme for cloud services based on the framework provided in the EU Cybersecurity Act (Regulation (EU) 2019/881), further referred to as the EUCS. Where reference is made to the EUCS this relates to version V1.0.319 dated May 2023.

NOREA acknowledges the need for a common high level of cybersecurity and resilience throughout the European Union and supports the efforts taken by the European Commission to this end. Critical comments and observations made in this evaluation are therefore intended to further improve the processes and operations in place to reach these goals in the context of a single European digital market.

NOREA, the professional association of IT auditors in the Netherlands, participates in the Dutch Online Trust Coalition (OTC) and endorses the OTC's consultation response.

Postadres
Postbus 7984
1008 AD Amsterdam

Bezoekadres
Antonio Vivaldistraat 2-8
1083 HP Amsterdam

E-mail en Website
norea@norea.nl
www.norea.nl

Overig
Tel: 00 31 (0)20 301 03 80
KvK-nr: 40537540
IBAN: NL02ABNA0475165403

In summary, our comments and observations relate to:

- **Cybersecurity Certification Framework**

The framework as laid down in the Cybersecurity Act is based on the Common Criteria / SOG-IS approach for product certification. Existing substantial differences in laboratory testing of products and the audit of services make the framework not suitable for certification of services.

According to Article 56 (2) of the Cybersecurity Act: "The cybersecurity certification shall be voluntary, unless otherwise specified by Union law or Member State law". Recent developments in other regulations and directives however show a tendency to mandate cybersecurity certification. Therefore in our opinion the requirements and processes in the scheme should be treated as if they are mandatory and a mandatory impact assessment prior to implementation of the scheme should be part of the framework.

Given the important role of the cybersecurity certification in other legal acts like among others NIS2 Directive, Cyber Resilience Act, e-IDAS2 and DORA, it is important to safeguard the consistency between these legal acts. Also opportunities for synergy and efficiency like harmonization of criteria across sectors and scope of legal acts and re-use of audit reports should be considered to reduce the compliance cost of CSPs and consequently reduce the price of cloud services.

- **EUCS scheme development**

Annex J of the draft scheme contains requirements that aim to safeguard the sovereignty of European cloud services (PUA: Protection against Unlawful Access). These requirements were included without a prior proper economic impact assessment. In the opinion of NOREA this faces the risk of disrupting the EU single internal cloud market. Furthermore the risk that the PUA requirements conflict with other international treaties and agreements like the General Agreement on Trade in Services (GATS) by the WTO, should be assessed.

The use of (European or international) standards is essential for the mutual recognition of the cybersecurity certificates and also for the effectiveness of all legal acts affected. Article 54 (1.c) of the EU Cybersecurity Act requires that the schemes shall at least include

references to international, European or national standards applied. Recital 69 of that same act states that the European cybersecurity certification schemes should be based on European or international standards. Requirements of certification schemes therefore should be based on existing standards. The draft EUCS scheme however contains important elements that are not standardized (e.g. Annex J) or are submitted for standardisation to CEN-CENELEC (the security requirements in Annex A and the Meta-approach). NOREA supports the role of CEN-CENELEC as it has a well established reputation and transparent governance structure.

There is a need to invest in the development of supporting tools and expertise. In accordance with the EU Cybersecurity Act the scheme currently requires Conformity Assessment Bodies to be accredited against ISO 17065 which is an obstacle for auditors that work in accordance with International Standards on Assurance Engagements (ISAE, issued by IAASB) to act as Conformity Assessment Bodies. As a result, the expertise of assurance auditors for cybersecurity certification is not being utilized, while the capacity is urgently needed. The IT audit profession has become an important factor in assessing and advising on the Cybersecurity Act, NIS-2 and DORA. In the Netherlands, a number of Master programs recognized by NOREA, ensure the influx of qualified IT auditors into audit firms and services. This model could be exemplary for other countries in the EU.

The Cybersecurity Act should include also other standards that will fit auditing of services and processes and especially the management processes. We think of standards like the ISO 17020, 17021 and international IT-audit standards of the IFAC/ISACA and IAASB-audit quality standard.

Overall the development of the EUCS is taking too long. Development by the Ad Hoc working group started in March 2020 and preparatory work was done by the CSPCert stakeholder group. An important factor in the delay was caused by the inclusion of sovereignty criteria. A discussion that started in October 2020 and still goes on until today. We recommend to separate the discussion on sovereignty from the completion of the scheme and give priority to completing the EUCS without Annex J.

General remarks

Evaluation of the Cybersecurity Certification Framework

Cybersecurity Act as basis for certification of cloud services

The certification framework presented in the Cybersecurity Act is intended to provide cybersecurity certification for ICT products, ICT services and ICT processes. The mutual recognition of certificates between the member states is an important condition. Preambles 68 and 69 of the Act name Senior Officials Group – Information Systems Security (SOG-IS) Mutual Recognition Agreement (MRA) as the most important model for cooperation and mutual recognition in the field of security certification. And therefore SOG-IS is considered an important building stone for the certification framework presented in the Cybersecurity Act. The impact of this decision however is that elements of SOG-IS, especially terminology, are used throughout the Act that are derived from SOG-IS.

SOG-IS is a product certification, performed by laboratories on products that have fixed specifications, behave consistently and in general do not change. If a product changes, a new product appears. Cloud services are volatile, are dependent on human behavior and adherence to procedures. They are tested by auditors for operating effectiveness. This is a different approach from the testing of products in laboratories.

Nevertheless the terminologies used in SOG-IS show a lot of resemblance with terminologies used in the audit of services. As an example the “assurance levels” defined in SOG-IS and used in the Cybersecurity Act have a completely different meaning in the audit of services. This leads to communication gaps that need to be bridged in the schemes.

Voluntary or mandatory?

According to Article 56 (2) of the Cybersecurity Act: “The cybersecurity certification shall be voluntary, unless otherwise specified by Union law or Member State law”. Recent developments in other regulations and directives however show a tendency to mandate cybersecurity certification. The EUCS is foreseen to play an important role in the implementation of the NIS2 Directive and also contribute to oversight and enforcement of, among others, the Cyber Resilience Act, e-IDAS2, AI-Act and DORA.

During discussions with ENISA and the European Commission on the proposed sovereignty requirements, the argument that certification is voluntary, is used to waive the need for an impact assessment. Given the importance of cybersecurity certification in the entire

regulatory context however, it is our opinion that cybersecurity certification should be treated as mandatory and therefore a thorough impact assessment on the schemes is needed prior to implementation.

Consistency with other legal acts

Over the years the European commission is launching a substantial number of Regulations, Act and Directives that each involve oversight of cloud service providers. As an example: apart from the oversight already in place, providers will now be faced with direct oversight by (or on behalf of) the European Supervisory Authorities (ESA's: EBA, EIOPA and ESMA). NOREA recognizes the importance of regulations and oversight. Equally important however in our opinion is the harmonization of requirements (criteria) and re-use of proof (audit) to reduce the administrative burden it imposes.

We call upon the European Commission to safeguard consistency among legal acts and improve harmonization and opportunities for synergy to keep use of cloud services competitive.

Evaluation of EUCS scheme development

Use of standards

The use of (European or international) standards is essential for the mutual recognition of the cybersecurity certificates and also for the effectiveness of all legal acts affected. Article 54 (1.c) of the EU Cybersecurity Act requires that the schemes shall at least include references to international, European or national standards applied. Reference is made to Regulation (EU) 1025/2012. Recital 69 of that same act states that the European cybersecurity certification schemes should be based on European or international standards. Requirements of certification schemes therefore should be based on existing standards. The framework does however not indicate for which elements of the scheme the use of (European or international) standards is mandatory.

At the beginning of the scheme development, an assessment is made by ENISA on what European standards can be used and for which parts of the scheme no suitable standards

are available. This assessment is an important starting point for the development of the scheme, however the gap assessment was not made public. In the case of the EUCS, ENISA started the scheme development by defining the criteria and the meta-approach which were afterwards submitted for review to CEN-CENELEC. In our opinion this was an important reason for the delay in the development of the scheme. For future scheme developments we recommend to perform the gap assessment together with industry experts from the Ad-Hoc working group or the SCCG and if gaps are defined, first explore the development of European standards before developing taylor made solutions by ENISA.

NOREA recommends to specifically define which elements of a scheme require mandatory use of acknowledged standards as well as the procedure to be used when standards are not available.

Supporting tools and expertise

Cybersecurity is a very volatile topic and threats and controls change almost on a daily basis. Currently the scheme contains a very detailed set of criteria that are generally considered to be state of the art. These criteria must also provide guidance both for parties responsible for cybersecurity of cloud services and auditors acting as Conformity Assessment Bodies for the cybersecurity certification. For an effective common level of cybersecurity and resilience throughout the European Union, the challenge is to reflect the volatility of the topic in the scheme's criteria and conformity assessment. We are concerned that for the execution of the scheme in the European Union insufficient tooling and expertise is available. We therefore strongly recommend to invest in the development of supporting automation, including AI and the training of auditors and monitoring of the work performed by CAB's.

The draft scheme in accordance with the EU Cybersecurity Act requires Conformity Assessment Bodies to be accredited against ISO 17065. This is an obstacle for auditors that work in accordance with International Standards on Assurance Engagements (ISAE, issued by IAASB) to act as Conformity Assessment Bodies. Allowing ISAE auditors to act as Conformity Assessment Bodies will not only increase the pool of expertise for EU cybersecurity certification, it will also lead to synergy with financial audits.

Finalization of the EUCS

The objectives of EU cybersecurity certification are too important to get delayed by political discussions. Development of the EUCS started in March 2020 and currently the implementation act has not been finalized. It is expected that when the Cybersecurity Act will celebrate its 5th anniversary in June 2024, not a single certificate will be delivered. It is simply taking too long.

On behalf of the NOREA-board,

Irene Vettewinkel-Raymakers,
Chair.