Position Paper

Response to ENISA consultation on the EUCS

Our reference:	EXCO-CS-21-022	Date:	5 February 2021
Referring to:	ENISA consultation on a candidate cybersecurity certification scheme for cloud services (EUCS)		
Contact person:	Áine Clarke, Policy Advisor, General Insurance	E-mail:	Clarke@insuranceeurope.eu
Pages:	4	Transparency Register ID no.:	33213703459-54

Summary

Insurance Europe welcomes the opportunity to provide input to the consultation on a candidate cybersecurity certification scheme for cloud services (EUCS). In principle, it is in favour of the establishment of a neutral and objective certification scheme for cloud services as this would increase and harmonise the level of security and reduce the obligations of operators, including insurers.

Insurance Europe therefore welcomes the development of a Europe-wide uniform certification scheme for testing and evaluating complex cloud services, and calls for full consistency with all European Union initiatives regarding cloud services, including the European Commission's proposal for a Digital Operational Resilience Act and its proposed supervisory framework applicable to information and communication technology (ICT) service providers.

A number of comments on the draft EUCS certification scheme can be found below (grouped by section):

Section 2: subject matter and scope

In principle, Insurance Europe does not oppose the recourse to or reuse of conclusions and evidence from already tested or certified ICT products, ICT processes and ICT services by external parties (analogous to Section 2). However, the general acceptance of certified products, processes and services carries the risk that the Conformance Assessment Body (CAB) will have to accept inappropriate and/or outdated standards or guidelines. The scope of recognised certifications should either be named and restricted, or the acceptance of other certifications should be expressly left to the CAB.

In addition, it cannot be concluded from the certifications of individual IT products, processes or services that the security and functionality of the entire cloud system is automatically guaranteed when the individual products, processes or services are operated together. Rather, the cloud system must be checked and evaluated in its entirety. The "basic certifications" can help the CAB to evaluate the cloud system, but an overall evaluation of the CAB is essential.

Sections 4: use of standards *and* Section 8: evaluation methods and criteria

Sections 4 and 8 list two families of assessment methods (ISO/IEC 17000 and ISAE 3000). The test methods of ISAE 3000 (here explicitly 3402) should not be permitted, as they were developed primarily to test service-based and accounting-relevant internal control systems and the focus is therefore on the examination of processes that serve the business management of companies. However, IT-specific aspects should be included in the assessment when certifying CSPs; aspects that are not adequately taken into account by the ISAE test methods.

In addition, an audit according to the ISAE standards is based on a description of the internal control system that the service provider itself provides. This means that the service provider has direct influence on the scope and depth of the assessment. The test method family ISAE 3000 should therefore be deleted from the EUCS draft.

- **Section 5: assurance levels** *and* **Section 6: self-assessment**

Insurance Europe advocates dividing the scheme into three levels, Basic, Substantial and High. However, it expressly does not advocate the possibility of a self-assessment of the CSP in the Basic level. This is likewise expressed by the authors of the draft in paragraph 6. However, in section 6 it is also pointed out that the possibility of self-assessments may be reconsidered in future releases of the scheme. A self-assessment should not be part of a certification scheme. The comparability of different cloud service providers (CSP) of the Basic level is therefore only possible to a limited extent or not at all. Thus, a basic requirement for a certification scheme (same basis for evaluating candidates) is unfortunately not given. At best, a self-assessment should serve as an information basis for the assessment body.

In addition, it is assumed in section 5 that, for the Basic level, "typical security requirements for services for non-critical data and systems" are sufficient. What are the typical security requirements? At the Basic level, the CSP only has to submit a self-assessment, if this is agreed in the present form. The "typical security requirements" thus depend heavily on the respective assessment of the CSP.

It is therefore not possible to compare different certifications in the Basic level. Practically, an informative value is not given. The users of the cloud service and their customers are led to believe that "uniform security and functionality requirements" have been met, but in fact it cannot be proven that the CSP fulfils these. A uniform standard is not possible in this way.

In addition, the classification of whether a cloud service:

- □ is suitable for critical or non-critical data and systems (Basic level); or
- □ is suitable for services for business-critical data and systems (Substantial level); or
- □ is suitable for mission-critical data and systems (High level)

should not be carried out by the EUCS. The determination of what a service is suitable for generally results from the use of a cloud service in the respective business case of the CSC. The classification can therefore only be carried out by the CSC and is very different. A general classification is thus not possible and should deleted.

Section 5 also assumes that it is sufficient if the evaluation depth for the Basic assurance level consists solely of inspection activities, based on a check for completeness and coherence of the provided documentation on processes and design by the CSP. In Insurance Europe's view, this is not the case. The correctness and completeness must be checked not by the CSP but by the CAB.

Section 5 also shows that the Substantial level differs from Basic in that on-site audit, including interviews and inspecting samples, are permitted in the Substantial level, which is apparently explicitly excluded in the Basic level. From the point of view of a CAB, this is not sufficient to be able to evaluate the safety and functionality of a service. A high-level presentation, as on page 22, and the general exclusion of on-site audits in the Basic level is not acceptable. The necessity and the scope of corresponding audits should be left to the CAB.

In addition, the requirements for the individual levels according to pages 22 to 23 are not acceptable. With regard to the scope of the Substantial level, this is already the standard for the evaluation of services and systems. These requirements should therefore already apply in the Basic level. Likewise, the scope at the High level should already be assessed by the CAB in the Substantial level. In Insurance Europe's opinion, the scope in the High level must be redefined. Based on the scope of the Substantial level, the High level should include the permanent and seamless review and monitoring of the performance of cloud services and their underlying individual processes, the implementation of proactive metrics and mechanisms for possible incidents and errors, and a more closely knit review of the performance criteria as well as the underlying control bodies. In principle, however, the CAB must be able to adapt the scope of the test individually to the respective design and criticality of the service at any time (at any level).

- **Section 7: specific requirements applicable to a CAB**

According to Section 7, it is only necessary for the High level that an accredited CAB must have the technical skills to be able to review the design and performance of penetration tests and the analysis of penetration testing activities. According to Insurance Europe's previous proposal to redesign the scope of tests in the individual levels, this ability should already have to be provided in the Substantial level of CABs. In addition, a penetration test should be either carried out by the respective CSP or there should be a possibility for the CSP to offer and perform an industry-sector-specific, re-usable or company internal standardised penetration test (to reduce cost and efforts for both the CSP and CAB). Both options should be based on industry standards (eg, Tiber or other relevant frameworks/cloud certification schemes), by which the results would be re-usable for all CABs, whether CAB internal or sector-wide. It is already possible for insurance companies to exercise certain information and audit rights regarding the cloud service provider via "pooled audits" together with other supervised companies. The same possibility should exist for penetration tests ("pooled tests"). Otherwise, the use of cloud technology would be made significantly more difficult or impossible, especially for small and medium-sized companies, due to economic hurdles. It should be ensured that pooled audits, once performed, can be used throughout the group at EU level.

Insurance Europe would also like to see a requirement that a penetration test for the CSP should be performed for all levels, starting with Substantial.

- **Section 12: certificate management**

Section 12 stipulates that, in addition to the CAB, the CSP, the NCCA and -in the event of a complaint- the National Accreditation Body, can initiate maintenance activities. It should be made clear that the initiating body only *informs* the relevant CAB of the complaint and it is the CAB that investigates the complaint. However, the responsible CAB should be able to decide in every case on the scope and depth of the required maintenance activities at the CSP.

- **Annex D**

The described documentation check cannot provide sufficient information on the function and security of the entire cloud system. Fundamental statements of the CSP, as well as corresponding security mechanisms, should be checked in an on-site audit by the CAB. An assessment performed only on the basis of a document check should not be permitted.

- **Annex F**

The information that a CAB needs within a certification process or processed within various reports varies greatly with the type of cloud service, the scope of the certification process, the desired certification level and the individual approach of the CAB. Therefore, the documents described in Annex F (F.2 Application Document, F.3 Audit Planning, F.4 Assurance and Evaluation Report, F.5 Review Report, F.6 Certification Package and F. 7 Maintenance Reports) should be included in the procedure as mandatory, but the CAB should be able to define the content and scope as well as the format of the documents itself. The scope of the documents depends heavily on how a CAB works. The descriptions in Annex F should therefore only be recommended and not binding.

- **Annex G.1.1**

An assessment and a reassessment of controls can also make sense at the Basic level and should not be explicitly excluded. The decision on the need for a (re)assessment should be left to the CAB. Similarly, a restoration assessment (G.1.3) should not be excluded in the Basic level.

For questions or comments on Insurance Europe's submission, please contact Mr. Christian Metzmacher (VdS Schadenverhütung GmbH, cmetzmacher@vds.de).

Insurance Europe is the European insurance and reinsurance federation. Through its 37 member bodies — the national insurance associations — it represents all types and sizes of insurance and reinsurance undertakings.

Insurance Europe, which is based in Brussels, represents undertakings that account for around 95% of total European premium income. Insurance makes a major contribution to Europe's economic growth and development. European insurers pay out almost €1 100bn annually — or €2.9bn a day — in claims, directly employ over 900 000 people and invest nearly €10 200bn in the economy.