Brussels, February 2021

BSA | THE SOFTWARE ALLIANCE'S FEEDBACK TO ENISA ON THE EUROPEAN UNION CYBERSECURITY CERTIFICATION SCHEME ON CLOUD SERVICES (EUCS)

The European Union Cybersecurity Certification Scheme on Cloud Services (EUCS) has the potential to be a powerful driver to improve cybersecurity risk management for cloud services across the EU. The EUCS market adoption will depend among others on its workability, its alignment with existing internationally recognized practices, and more importantly, its ability to provide a single European benchmark for cybersecurity requirements and operating rules for cloud service providers (CSPs) across Member States. BSA welcomes the opportunity to provide feedback to the ENISA Ad Hoc Working Group on the draft version of the EUCS candidate scheme. Given the complex nature of the scheme and the allotted length for responses in the online questionnaire, we respectfully submit additional feedback with expanded answers.

BSA | The Software Alliance[1] supports the inclusion in the EUCS of a supply chain holistic approach for CSPs to secure development processes, and have the ability to adapt to changes in the security environment. BSA has developed a Framework for Secure Software to offer an outcome-focused, standards-based risk management tool to help stakeholders in the software industry – developers, vendors, customers, policymakers, and others – communicate and evaluate security outcomes associated with specific software products and services.

Specifically, the Framework is intended to be used to:

a) help software development organizations describe the current state and target state of software security in individual software security products and services;

b) help software development organizations identify opportunities for improvement in development and lifecycle management processes, and assess progress toward target states;

c) help software developers, vendors, and customers communicate internally and externally about software security; and

d) help software customers evaluable and compare the security of individual software products and services.

More details on BSA's position on these requirements can be found in BSA's Secure Software Framework (https://www.bsa.org/reports/updated-bsa-framework-for-secure-software).

(BSA responses to applicable questions appear in blue.)

[1] *BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.*

BSA's members include: Adobe, Akamai, Atlassian, Autodesk, Bentley Systems, Box, Cloudflare, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

2. Participant Profile

2.1 Achieved Certifications and Intentions

2.1.1 If you are a CSP, does your company or entity is already compliant with existing certifications and standards?

- International standards (ISO, IEC, ITU, ...)
- European national schemes (C5, SecNumCloud, ENS, ...)
- Non-European national certifications (NIST, IPA, ...)
- Domain-specific certifications (PCI DSS, ...)

Clarification: BSA members collectively use all the certifications and standards listed above but that not all members are compliant with all these existing certifications and standards.

*2.1.2 The implementation of this draft EUCS candidate scheme will be voluntary by nature.
Do you intend to use the EUCS scheme?

- Yes
- No

*2.1.3 Would you consider using the draft EUCS candidate scheme to:
You can select more than one

- Require or recommend certification
- Use certified cloud services
- Certify one or several of the cloud services your company provides
- Develop certification activities as a Conformity Assessment Body (CAB)

2.1.4 What level(s) of assurance would you target for the cloud services you would want to have certified?

- Basic
- Substantial
- High

2.1.5 Can you please elaborate on your choice?
250 character(s) maximum

Three tiers help organizations address in a flexible way the variety of cloud services, intended uses by different types of customers, different risks and threat levels faced by customers and CSPs. Clearer definitions and concepts would be welcomed.

Expanded answer:
BSA members are among the world's most innovative companies, creating widely adopted software and cloud solutions that spark the economy and improve modern life. Members' cloud services are consumed in a wide variety of contexts from small businesses to governments, from low risk to highly sensitive use-cases.

Defining three tiers of assurance levels will help address the variety and different uses of cloud services by different types of customers, the different risks and threat levels faced by customers and providers of cloud services. Having different levels of assurance gives organizations flexibility in

apply the appropriate level of security to their cloud business case. The tiering could be improved by bringing further clarity to some areas and concepts. For example, section D.3 'Developing the audit plan' in the Level Basic Assessment states that the evaluation depth shall be defined by a predefined audit plan; however, the current draft does not detail what that predefined audit plan should entail.

The tiering also helps to provide a higher level of security for sensitive business activities while avoiding forcing expensive, high security requirements on to low risk business cases. This risk-based approach could be further emphasized more consistently throughout the scheme. It would also be important to clarify how these assessments operate with other assessments done outside the EUCS, to avoid duplicating efforts stemming from the EUCS and other relevant standards and certifications.

*2.1.6 What do you foresee as being the biggest challenge to achieve the future EUCS certification?
250 character(s) maximum

Challenges relate to cost complexity of the certification process, duplication with national and internationally-accepted certifications/standards, lack of clarity on mutual recognition and concurrence with national schemes in public procurement.

Expanded answer:
We welcome the fact that the EUCS has been built with existing widely adopted, internationally recognized, risk management based, voluntary standards as reference, such as ISO/IEC 27001 and SOC 2. Such certifications allow for the evaluation of providers according to consensus criteria based on well-established industry best practices. We also welcome that some technical requirements are based on two existing single-level evaluation methodologies or certifications, Germany's BSI C5 and France's ANSSI SecNumCloud, which have both achieved some market acceptance. Applying existing cloud security standards is an effective and efficient way of assuring the security of cloud services and allow different providers to compete on the basis of their security practices. Indigenous or overly prescriptive standards can greatly increase the cost of compliance and oversight without adding to security outcomes. Many BSA members have successfully obtained certifications against standards specific to cloud security and privacy as well as more broadly focused on information security. Both effectively demonstrate to clients the robustness of security controls and organizational security practices.

It will be important to ensure that the EUCS is interoperable and integrated in a harmonized way with the many and various cloud certification approaches already in place around the world and in EU Member States in order to limit unnecessary burdens on cloud service providers and not confuse the existing level of customers' confidence. For instance, the EUCS could incorporate C5 and SecNumCloud as security objectives by reference in order to further align with these schemes and eventually phase them out as the EUCS is adopted at EU level. Having a single certification scheme recognized across the EU will be attractive to cloud service providers and will also drive market adoption of the EUCS. In the event where existing national certification schemes were not withdrawn, there should be equivalence or mutual recognition between the EUCS and national schemes such as C5 and SecNumCloud, barring specific additional requirements. This would ensure that there are no unnecessary market access barriers created by concurrent certification requirements within the EU.

BSA also supports the proposed EUCS scheme's recognition of the shared responsibility model of cloud services. The principle of shared responsibility should be the gold standard to recognize the different responsibilities in cloud operations, and hold entities responsible for the aspects of the environment over which they can be held accountable. Applying security requirements to CSPs for parts of the cloud ecosystem they do not have access to can have counter-productive outcomes for security and privacy.

In order to improve its workability, the scheme could further support and encourage the reuse of conclusions and evidence from previously audited or certified ICT products, ICT processes, and ICT services. Repeated audit and certification activities on already scrutinized cloud services is wasteful, adds to the regulatory and oversight burden of a scheme, and distracts security staff from other security activities. Using widely adopted, international standards and allowing the reuse of security conclusions and certifications will likely greatly increase the adoption and success of the scheme by significantly reducing the cost of compliance.

Other challenges that could arise include a lack of suitably qualified auditors available to assess cloud services (particularly at the start of the program) and the application of any additional, unnecessarily burdensome controls applied beyond those in the widely adopted international standards.

Last but not least, timing will be of the essence. It would be helpful for the guidance to be in place before the scheme comes into force. This would provide additional clarification on the scheme's implementation process and allow organizations to prepare and dedicate resources accordingly. In addition, both the Cybersecurity Act (Article 56) and the Proposal on measures for a high common level of cybersecurity across the Union (NIS 2) in its Article 21 specifically foresee the possibility for Member States and the European Commission to make certification schemes mandatory. It is therefore paramount to ensure that as those legislative requirements become a reality, tools and mechanisms such as the EUCS are available and reliable for organizations to build compliance.

*2.1.7 Can you please indicate your reasons for not using the draft EUCS scheme? What to your opinion would be needed for you to use the EUCS scheme?
250 character(s) maximum

3. Objectives of the Scheme

3.1 Impact of the EUCS Scheme on EU Market Conditions

The draft candidate EUCS presents the following proposals to enhance the market conditions for certified Cloud Services (both under the EUCS scheme and future schemes):

- An EUCS certificate will be valid throughout the entire European Union;
- An EUCS certificate opens to composition with future schemes developed by ENISA under the European Cybersecurity Certification Framework;
- The certificates issued will also include a label that is associated to the EUCS scheme;
    - The label will be designed in a harmonised and clearly recognisable way across all EU cybersecurity certification schemes;

- The label will associate a unique URL and QR-code to the certificate. The URL and QR-code will provide access to the relevant publicly available information about the certified service, and other related information regarding the Cybersecurity Certification Framework under the ENISA website dedicated to European cybersecurity certifications.

*3.1.1 Do you believe that the aforementioned proposals will have a positive impact on market conditions for the certified Cloud Service, both under the EUCS and future schemes?

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

3.1.2 Please provide any further comments you might have on the impact that the draft EUCS candidate scheme may have on the market conditions and/or indicate any information that you think would be necessary.

250 character(s) maximum

The EUCS should be risk-based, outcome-focused, tech-neutral, adaptable, workable, reuse existing security conclusions, be interoperable with internationally recognized schemes, avoid mutually incompatible country-specific certification schemes.

Expanded answer:

Overall, the EUCS can have a positive impact on the market, provided it clearly aims to (1) promote interoperability and avoid mutually incompatible country-specific certification schemes, (2) promote a risk management approach to cloud security, and (3) provide confidence to customers in the integrity and security of cloud services. The more the scheme is (1) risk-based, (2) outcome-focused, (3) technology neutral, (4) adaptable, (5) is able to reuse existing security conclusions and certifications, and (6) interoperable with existing internationally recognized certification schemes, the stronger market adoption will be.

Workability will be key to the adoption of the EUCS. As an illustration, Annex A lists approximately 600 requirements across assurance levels - Basic, Substantial and High. This could create significant compliance burden and prohibitive costs, in particular for SMEs, to prepare and implement the necessary controls prohibitive, lowering the attractiveness of the scheme despite its voluntary nature and market relevance.

BSA members value the opportunity for CSPs to compete on the basis of their security practices. The design of the controls associated with assurance levels could contribute to furthering trust and encourage innovation in the market, by coupling similar controls for all levels with different methods to satisfy each level of assurance.

4. Understanding the Key Concepts of the Scheme

4.1. Assurance Levels - Chapter 5

The Cybersecurity Act defines three assurance levels: 'basic', 'substantial' and 'high' that do not have to be covered by all schemes. The EUCS scheme matches these three levels, in order to satisfy the diverse needs of the industry, users and regulators.
There is no indication of an immediate need to go beyond three assurance levels in the scheme, but more levels could be added in the future.
The definition of the levels has been a key issue in the scheme. It was the main focus of the limited survey last summer, and the following questions are an essential part of this survey.

4.1.1 According to the generic description of the levels provided in the Cybersecurity Act, and on the detailed descriptions provided in the EUCS Scheme, which level(s) do you believe are relevant for Cloud Services?

- Only the 'substantial' level, which represents most use cases for cloud services now and in the future
- Only the 'high' level, for which certification is essential to trust CSPs now and in the future
- Both the 'substantial' and 'high' levels, to cover both mainstream use cases and highly sensitive use cases now and in the future
- Both the 'basic' and 'substantial' levels, as most services are not sensitive at all, so the limited guarantees of the Cybersecurity Act's 'basic' assurance level is sufficient for these
- All three levels, because today and in the foreseen nearby future there should be cloud services of all kinds, facing very different security challenges, and the scheme should follow

4.1.2 Which level(s) do you believe are the most relevant for your industry/vertical, and why (criticality of business or mission data, regulatory obligations, etc.)?
250 character(s) maximum

Cloud services are used in many contexts from SMEs to governments, from low risk to highly sensitive use-cases. Decisions on assurance levels should be based on rigorous risk management, can change over time as threats and business practices evolve.

Expanded answer:
Members' cloud services are consumed in a wide variety of contexts from small businesses to governments, from low risk to highly sensitive use-cases, depending on the criticality of the data. Decisions on security assurance levels should be based on a rigorous risk management process and can change over time as the threat environment and business practices evolve.

BSA supports the proposal to have three levels of assurance. All three levels are relevant as organizations across all industries and sectors use cloud services (whether at infrastructure, platform, and/or application level). Divergence between horizontal requirements and sector-specific requirements should be as targeted as possible and adopt a risk-based approach to reflect the different risks and threat levels specific to each sector/organization.

There are obvious cases that require higher assurance levels, but even within high risk verticals, and organizations undertaking high risk activities, there are business cases for cloud services that do not require high security assurance. Similarly, there may be business cases within low risk industry

verticals that require a high level of assurance. Organizations should have the flexibility to apply the right level of security assurance to the right cloud service requirement. The EUCS scheme should be careful about applying a blanket security requirement to entire industry verticals to avoid burdening companies with unnecessary costs and stifling innovation. Instead, where possible, it should provide advice on threat, risk management processes and security advice, and allow organizations to apply the right assurance level to business processes.

Similarly, the use of cloud services should be consistent with the additional legal and regulatory obligations that apply to cloud services customers, as to not restrain their ability to adopt technologies that will improve their security posture and to treat cloud computing in a similar way to outsourcing activities. This is in particular relevant as the EU currently debates legislative proposals that will have horizontal impact (NIS 2.0 proposal) and vertical impact (Proposal for a Directive on Operational Resilience in the Financial Sector (DORA)) on security requirements for CSPs and their customers.

4.2 Certificate Lifecycle

The Cybersecurity Act requires "continued compliance" to the scheme requirements, a reminder that certification is not a one-shot activity, but a lasting process. The EUCS scheme defines certificate maintenance mechanisms, in particular Annex G, as well as compliance monitoring and vulnerability and nonconformity handling mechanisms in Chapters 11 to 14.

4.2.1 Regarding maintenance, the EUCS scheme made a choice, but alternative choices are possible. Which approach do you believe is the most appropriate for cloud services?
at most 3 answered row(s)

	A full assessment is required every year	A full assessment is required every 3 years, with a partial maintenance assessment every year between full assessments, essentially to cover changes in the cloud service and threat environment over the previous period	A full assessment is required every 3 years, with a partial maintenance assessment every year between full assessments, covering changes and also including a full audit of the operating effectiveness of the CSP's controls.
Basic level		X	
Substantial level		X	
High level		X	

4.2.2 Please indicate if you have further comments:
250 character(s) maximum

At the high-level, we recommend a three-year frequency, in keeping with standard practice under ISO certification schemes.

Expanded answer
At the high-level, we recommend a three-year frequency, in keeping with standard practice under ISO certification schemes. This would help organizations to optimize the use of their resources and workforce at the service of their security objectives. Updates to processes in services and major changes (technical or to the ISMS) happen at such a pace that they should not automatically trigger

non-conformity and require recertification, at the risk or rendering the scheme non-workable; rather, the certification should be valid on a time span.

4.3 Subservices and Composition

4.3.1 Many cloud services use subservices to implement a part of their services, for instance when a SaaS service is implemented on top of a IaaS or PaaS cloud service. The EUCS scheme requirements apply equally for all cloud services, on the entire stack of services, so subservices need to be considered, typically by leveraging existing reports and certificates.
Which aspects are essential to you?

- The criteria should be the same for all services, independently of their implementation (with or without subservice providers)
- The CSP must have processes in place to evaluate and monitor its subservice providers
- Subservice providers must provide documentation with a level of assurance that is similar to the assurance level targeted by the CSP
- The documentation from subservice providers must be audited for compliance with the EUCS requirements
- The CABs shall base their audit on their professional judgement when the assurance documentation is not directly mapped to the EUCS requirements
- The analysis should be much easier when a subservice provider holds an EUCS certificate for its service
- An EUCS-certified infrastructure or platform provider should have the option to provide audited documentation to help their customers get certified themselves

4.4 Security Profiles

4.4.1 The EUCS scheme is a horizontal scheme, but specific industries and verticals may have additional requirements. The scheme includes a provision for the definition of security profiles, that would allow to do just that.
Which aspects would be essential to you?
at most 3 choice(s)

- It is important to allow industries and verticals to define security profiles
- Security profiles should only be allowed to add requirements, without changing existing requirements or assessment methodologies
- Cloud services should have the ability to claim compliance to security profiles in addition to the EUCS scheme
- Security profiles should be adopted by the ECCG
- EUCS security profiles should be evaluated and certified, like EUCC's protection profiles

4.5 Transition

After the present review, the scheme will be finalized and delivered to the European Commission after a formal consultation of the ECCG. The European Commission will then draft an Implementing Act, to be adopted by a committee of Member State representatives.
In parallel to this work, ENISA will, with the support of working groups and the ECCG, prepare for the adoption of the scheme, in particular through the development of guidance.

After the adoption of the Implementing Act, some work remains before issuing certificates. In particular, CABs have to be accredited, and CSPs have to prepare their cloud services for certification.

4.5.1 The adoption covers that time when all the EUCS stakeholders get ready. How long do you expect the adoption period to last?

- Under one year
- Between 12 and 18 months
- Over 18 months

4.5.2 Once EUCS certificates start being issued, a transition period starts to allow cloud services assessed under a national scheme to get certified under the EUCS scheme.
Are you considering to migrate from a national scheme?

- Yes
- No

4.5.3 How long do you expect the transition period to last?

- Under one year
- Between 12 and 18 months
- Over 18 months

4.6 Assessment Methods

The scheme supports two methods: one for assurance level Basic, which provides limited assurance, and one for assurance levels Substantial and High, which provides reasonable assurance (both concepts from the ISAE handbook, which are defined in the scheme).
The scheme does not explicitly support well-known methods like ISO/IEC 1721 or ISAE3402, because they are too different to be directly supported in the scheme. However, the assessment method for assurance levels 'substantial' and 'high' has been designed to be easy to combine with either of these methods. Guidance will be developed to help CSPs prepare for such combined assessments and to help CABs perform them.

4.6.1 Basic Assessment Method - Annex D

4.6.1.1 The assessment method for the Basic assurance level is based on a self-assessment following a standardized checklist, which is then audited by an accredited CAB.
Which aspects are essential to you?
at most 3 choice(s)

- A self-assessment is the proper basis for the Basic assurance level, provided that the results are audited
- Even for the audit of a self-assessment, it is important that the CAB be accredited as having the same competencies that are required for performing a full audit
- The Basic assessment method is based on standardized checklists
- The CAB has the ability to make specific requests to the CSP
- There are regular synchronization points between the CAB and the CSP during the assessment
- The CAB and the CSP meet at least once in the CSP's premises

4.6.2 Substantial-High Assessment Method - Annex C

4.6.2.1 The same assessment method is used for levels Substantial and High, and the difference between the two levels come from specific requirements for level High, from the different level of risk associated to each level, and from specific authorization requirements for CABs at level High. Which aspects are essential to you?

at most 3 choice(s)

- The consistency of assessment methods is essential for comparability and exploitation of results
- Assurance level High should use a stricter assessment method
- A risk-guided assessment method allows proper gradual increase between levels Substantial and High
- Specific authorisation procedures by the NCCA are required to ensure that CABs have the proper competences for level High

4.6.2.2 The assessment method is designed to be efficiently combined with other assessment methods such as ISAE 3402 or ISO/IEC 27001, and it will introduce transition paths from existing national schemes. Which aspects are essential to you?

at most 3 choice(s)

- Combining an EUCS assessment with an ISAE 3402 audit
- Combining an EUCS assessment with an ISO/IEC 27001 audit
- Transitioning to an EUCS assessment from a national scheme
- Combining with or transitioning from other schemes

4.6.2.4 Please Indicate if you have any further comments:

250 character(s) maximum

Third party audits are common practice. Similar requirements in the EUCS should not create repetitive or duplicative requirements, nor should they go beyond what is currently accepted in terms of audit and on-site inspection.

Expanded answer

In substantial and high levels, third party audits are common practice. Similar requirements in the EUCS should not create repetitive or duplicative requirements. They should not they go beyond what is currently accepted in terms of audit / on-site inspection or vulnerability handling, nor in terms of the level and type of evidence to be provided and their public availability. Third-party testing should remain independent, and operated in a coordinated and confidential manner, not to run against non-disclosure agreements currently in place with auditors. The suggested documentation management (evidence) requirements, by which CABs should retain access to records for at least seven years after the expiration of the certificate, go beyond exiting practice and raises concern with regards to confidentiality. These commonly accepted practices will not only help the market adoption of the EUCS, they should also be reflected in current legislative discussions as mentioned above (in particular, NIS 2.0 and DORA proposals) to avoid overlap and overly stringent requirements at the expense of sound risk-management approach.

In order to increase its workability, the EUCS could also expand the means by which to meet audit requirements. For many CSPs, it may be impossible to provide on-site audits given the number of

customers most processors have. In addition, the scope of such audits may also involve accessing data and systems that other controllers similarly utilize from a CSP, which would be in direct conflict with certain confidentiality agreements. The EUCS could recognize that auditing requirements could be achieved by virtual audits, or by offering to make compliance certifications/third party audit reports available to the customer.

Security Controls - Annex A

The Cybersecurity Act defines a list of requirements that is quite innovative. In the initial part of the development, and in the CSP-CERT study that preceded the work on the actual scheme, no existing set of evaluation criteria has been found to meet all of the scheme's requirements.
The scheme does not define controls, but requirements on the controls to be implemented by the CSP. These requirements come from a variety of sources.
We have used the following sources:

- The C5 criteria defined by BSI; which form most of the baseline for the 'substantial' level and contribute to the definition of the 'high' level through their "additional criteria";
- The SecNumCloud requirements, as defined by ANSSI, which complement C5 for the 'substantial' level and are also used to define the 'high' level;
- The requirements defined in the CSP-CERT report; and
- Some requirements from the ISO/IEC 27000 family of standards

The requirements are grouped in 20 categories, and the survey contains questions that allow you to react to every category.
One of the hardest challenges has been the addition of levels. Most sets of criteria are defined with one level of assurance level in mind. In order to define three levels, we often had to "split" an apparently simple criterion into several requirements, then assigned to different levels. This leads to a large number of requirements, but in the end, for instance, the requirements at level Substantial are very similar to those of the C5 criteria.

5.1 All categories and security objectives apply to all levels in the current proposal, with different requirements:

- This is a sound principle
- This is too demanding for the Basic level, so some security objectives should apply only for levels Substantial and High
- This is not demanding enough for the High level, so some security objectives should apply only for level High

5.2 In addition to traditional ISMS requirements, the scheme includes objectives and requirements related to the security features of the cloud service itself:

- There should be more requirements like this
- The requirements about the cloud service are about right
- There are too many such requirements

5.3 About pentesting, the current approach for level High is to mandate regular pen testing by qualified experts, involving external providers, and following a multi-year program reviewed by the CAB together with the test results.

From you viewpoint, what aspects are essential in a scheme?
at most 3 choice(s)

- The competence of pen testers is recognized
- The pentesters are independent from the product teams
- The pentesters are external providers
- The CAB reviews the pen test results
- The CAB reviews the pen test programme
- The CAB (or an accredited tester) participates to some of the pen tests as part of the audit
- The CAB (or an accredited tester) performs the pen tests as part of the audit

5.4 Also for level High, there are controls mandating automated monitoring of some controls, as a first step toward continuous assessment.
What statements feel right for you?
at most 3 choice(s)

- Continuous assessment is an important mid- or long-term goal for certification of cloud services
- Automated monitoring is an essential first step toward continuous assessment
- Automated monitoring can be implemented today by CSPs
- Automated monitoring remains a challenge for most CSPs
- The automated monitoring requirements in EUCS are appropriate
- Automated monitoring requirements should be generalized in EUCS for level High
- Automated monitoring requirements should also be present at level Substantial
- The automated monitoring requirements are too difficult, even at level High

---

For more information, please contact:
Isabelle Roccia
isabeller@bsa.org