Review of the Cloud Service Provider Certification self-regulatory group ("CSPCERT") Public Consultation on Milestone 1 and Milestone 2

A. Summary

The CSPCERT working group is exploring the possibility of creating a European Cloud Certification scheme in the context of the Cybersecurity Act. The consultation makes the case for establishing a certification for European Cloud Service Providers ("**CSP**") based on commonalities between the varying security standards which are currently in force. Any certification programme which breeds customer trust in the industry should be welcomed but only if assessment and certification are governed by CSP in conjunction with CSPCERT as leaders and innovators in the sector. Members are therefore invited to review the set list questions set out in the accompanying questionnaire.

B. Background

1. The CSPCERT working group have prepared a consultation on the creation of a European Cloud Certification Scheme with comments now open to the Public. We have until 3 February 2019 to provide a response to the consultation if the form outlined by the CSPCERT.

2. The working group was formed in December 2017 in preparation for the Cybersecurity Act which proposed a number of enhanced measures to deal with the growing threat of cyber-attacks across Europe. The final form of the Cybersecurity Act was agreed between the European Parliament, Council and Commission on 10 December 2018.

3. One of the key proposals of the Cybersecurity Act was the introduction of a framework for European cybersecurity certificates for products and services which will be recognised across the union. CSPCERT is focused on creating a European cybersecurity certificate for cloud services for the benefit of CSP and customers.

4. The consultation is keen to recognise the importance of current security standards and seeks to ensure a certification system compatible with all of the leading security standards. Milestone 1 addresses what the required security standard should look like for CSP in order to be awarded certification.

5. Milestone 2 focuses on the application and assessment process a cloud service provider should be required to complete in order to be accredited as compliant with the standards set out in Milestone 1.

6. Much like the introduction of the Cybersecurity Act, the fundamental purpose of the CSPCERT working group is to create greater customer confidence in the security implemented by CSPs and the cloud service industry as a whole.

C. Comment

Security Standards

7. Let's first take the issue of "a European standard". In respect of cloud specific security requirements there is no uniform set of rules. While there are inevitably "commonalities" in the high-level categories outlined in Milestone 1, within each of these categories are subtle differences at a more granular level. For example, in respect of 'Information Security Policies, objective ISP3 states "the CSP must communicate all information security policies to both its internal and external stakeholders (e.g. cloud service customer)".

8. While ISO 27002 states that policies should be communicated to "employees and relevant external parties" which could be argued includes customers. The C5 does not appear to mention the disclosure of policies to customers and focuses more on the disclosure of audit outcomes.

9. CSPCERT, in respect of their 'security requirements' need to strike a balance between not imposing additional obligations on a CSP who is accredited by one standard but not another and on the other hand simply rubber stamping any CSP through the certification process who has already been accredited by one of the security standards outlined in the 'methodology'. The first approach may deter some CSP from applying particularly against the backdrop of Brexit (discussed in more detail at Section E) and the latter may serve to devalue the significance of the CSPCERT.

10. While the current draft of the CSPCERT security requirements are based on the latest security standards how frequently will the CPSCERT security requirements be reviewed in order to ensure they continue to meet the standards set out in other European and international security standards?

Assessment

11. There are several forms of assessment listed within the consultation papers but only two seem credible from a CSP practicality perspective. Evidence based conformity assessment being the main method, where by the CSP investigates if they meet the security requirements for certification and the outcome is in turn reviewed by CSPCERT authority. CSP understand the market, their business and future innovations better than any third party and therefore it makes commercial sense that the initial investigation is conducted internally.

12. The suggestion of third part assurance testing not only proposes to be more costly for CSP but will encompass more employee time dealing with the audit process. In any event, many CSP will already have relevant security accreditations (such as those set out in Milestone 1) which would have required them to have undergone a rigorous audit.

13. We consider that CSPCERT status should be awarded to a CSP if they meet the security requirements for period of three years before a further assessment is required. Three years is a sufficient period of time to keep up with the fast paced developments in cloud services but without being too onerous on CSP.

14. Continuous monitoring for critical services does seem to be a sensible approach especially if the duty remains on the CSP to self-report any issues or fallings against the CSPCERT security requirements.

D. Structure of the Consultation

15. As already discussed the consultation is split into two papers, Milestone 1 and Milestone 2 which are set out as follows:

Milestone 1

16. After providing some background and introductory remarks the consultation under the section entitled "Methodology" outlines the documents used as an input for the security objectives as follows:

    a. Study on Certification Schemes for Cloud Computing (SMART 2016/0029);
    b. ISO 27002, 27017, 27018;
    c. ENISA Cloud Computing Schemes Metaframework;
    d. BSI C5; and
    e. SecNumCloud.

17. The working group have listed the key commonalities between these standards into a series of 12 categories as follows:

    a. Information Security Policies, Personnel & Training, Asset Management, Identity and Access Management, Cryptography and Key management, Physical Infrastructure Security, Operational Security, Communications Security, Procurement Management, Incident Management, Business Continuity and disaster recovery, Compliance, Security Assessment, Interoperability and Portability, System Security and Integrity, Change and Configuration Management and finally Risk Management.

18. The paper then works through each of these categories providing a high level overview of the standards required by a cloud service provider in order to achieve the requisite level for CSP Certification.

19. Annex 1, provides a high level gap analysis of each category against each of the standards listed at paragraph 15 above.

Milestone 2

20. After providing some background and introductory remarks the consultation under the section entitled "Conformity Assessment Methodologies" outlines the potential approaches to assessment as follows:

    a. ***evidence based conformity assessment –*** where the cloud service provider carries out a self-assessment which will then be subject to a third party review.
    b. ***third party insurance*** - this refers to a third party audit to ensure the CSP is complying with the security requirements before being certified;
    c. ***continuous monitoring –*** this will only apply to critical infrastructures, financial networks and systems which require continuous monitoring and certification.

21. The paper then discusses each of these "conformity assessment methodologies" in more detail.

E. Additional

22. Another factor which needs consideration is Brexit and the uncertainty surrounding the United Kingdoms scheduled withdrawal from the European Union on 29 March 2019.

23. In remains to be seen whether UK based cloud service providers will want to sign up to a European Certification programme which may incorporate elements of European standards they would not ordinarily need to meet. Particularly, as the ISO standard that most UK companies base their standards upon are recognised worldwide and could be vital in any future trade agreements away from Europe.

24. Alternatively, this form of certification may provide cloud service providers with some reassurance that they can keep and attract new customers from the European Union despite Brexit.

25. It remains to be seen which of these approaches cloud service providers adopt and much may depend upon the terms of any agreement. The consultation also fails to elaborate on whether a CSP qualifies for certification based on being a European registered company or because they provided cloud services to European companies.

F. Conclusion

26. The draft consultation can be a positive step for CSPs if an appropriate certification methodology and agreed security requirement can be established and maintained.