afme/
Finance for Europe

Position Paper – FINAL DRAFT

Considerations for an EU Cloud Certification Scheme for Cloud Service Providers

7 February 2021

Introduction

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to engage in discussion on the development of an EU Cloud Certification Scheme (CCS) for Cloud Service Providers (CSPs).

We believe that the adoption of new technologies, such as cloud, can make the EU financial sector more innovative, competitive, and increase resilience. We believe that the proposal for a CCS for CSPs can alleviate some of the regulatory burden placed on financial entities by increasing assurances on the security and controls of cloud services provided by CSPs. The proposed CCS for CSPs also provides an opportunity to enhance understanding and transparency between financial entities, regulators, and CSPs, and can complement other related guidelines and proposals that exist within the EU[1].

We believe that the following recommendation will be important for ensuring that the CCS for CSPs can bring benefits to the financial services sector:

- **An EU CCS for CSPs should aim to increase transparency and trust between CSPs and financial entities.**
  - Currently, CSPs and financial entities use different security controls based on their respective sector, underlying processes, or regulatory requirements. This means CSP on-boarding by financial entities remains a lengthy and complex process. Voluntary certification schemes could promote common standards between CSP and financial entities which in-turn could increase the uptake of cloud services in the EU. It may also alleviate some of the cost and complexity financial entities face when using cloud services.
- **An EU CCS for CSPs should seek to become an industry standard within the EU, and globally, for CSP qualification and certification.**
  - There are currently well established global and regional industry recognised certifications for CSPs (e.g. ISO/IEC, NIST, IOSCO). Because the EU CCS for CSPs only references a limited number of international standards (ISO/IEC) it is unclear how the scheme will align with internationally recognised standards for CSP certification. We recommend the proposed EU CCS for CSP includes additional references to international standards as well as where alignment is achieved or is different, to provide clarity to CSPs and financial entities using international standards. This will also support cross-border activity by enabling mutual recognition between certificates in use.
- **Financial entities should have flexibility in selecting an appropriate level of assurance ('basic', 'substantial' or 'high') for cloud services, even for critical activities.**
  - This would be compatible with a risk-based approach, where financial entities have flexibility in managing their risks, rather than assuming a 'high' level of assurance should be required for all critical activity. While a high level of assurance guarantees a certain level of security and control from a CSP it does not cover for all risks or consider the additional level of security provided by the financial entity. Therefore, a critical activity which has received a 'high' level of assurance by the financial entity may not always require an equal amount of assurance by the CSP.
- **We recommend that some of the scope, terms, and definitions within the CCS for CSPs are clarified to provide transparency to CSPs and financial entities on what assurances are provided under the CCS.**

[1] EU Cybersecurity Act (2018); EBA Outsourcing Guidelines (2019); EBA ICT and security risk management Guidelines (2019); Standard contractual clauses for CSPs (2020); EU Cybersecurity Strategy (2020); Digital Operational Resilience Act (current)

- The main purpose of the CCS should be to increase the uptake of cloud services in the EU by alleviating some of the cost and complexity financial entities face when using cloud services. In particular, we welcome efforts where the proposed CCS for CSPs could enable CSPs to help financial entities meet their current and future regulatory requirements when using cloud services (e.g. EBA Outsourcing Guidelines, EBA ICT Guidelines, DORA);

- **We recommend that certification remains voluntary.**
  - A voluntary approach to certification will provide flexibility to both CSPs and financial entities to select the best possible certification scheme, even outside the EU, to meet respective requirements (e.g. security, controls or regulatory) in a way that is principles and risk based. A voluntary approach would increase transparency, security, and trust between CSPs and financial entities. A mandatory approach to certification risks financial entities needing to adopt a specific certification scheme which may not be best in class, leading to an inefficient use of resources to comply with the scheme. This could undermine trust and ultimately security between CSPs and financial entities.
- **We recommend the EU CCS for CSPs incorporates regular reassessments to ensure that it remains adequate over time** (e.g., to changing customer controls and threat modelling).

Our detailed assessment is provided below. We look forward to continuing to support this important initiative.

Section 2: Participant Profile

The Association for Financial Markets in Europe (AFME) represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia.

AFME is registered on the EU Transparency Register, registration number 65110063986-76.

Section 3: Objectives of the Scheme

- Further clarity is required in the text that the proposed CCS for CSPs is intended for providing assurance of production systems (rather than testing, or research and development, systems and environments).
- Further clarity is required on the use of the term 'user'. Is it currently unclear if the team refers to cloud service *customers* (e.g. a person or team responsible for managing the CSP contractual relationship) or cloud service *consumers* (e.g. a person or team using the CSP services). We recommend the term '*user*' in the context of this proposal only refers to cloud service *customers* who will be the primary users of the scheme (e.g. 4.1. Assurance levels chapter 5). We note that cloud service consumers are also referenced in the proposal, specifically for provisions considering documentation provided by CSPs (e.g. 5.5. security control categories). We recommend that in this case 'user documentation' is referred to 'cloud service consumer documentation'.

Section 4: Understanding the Key Concepts of the Scheme

- An EU CCS for CSPs should seek to become an industry standard within the EU and globally for CSP qualification and certification. There are currently well established global and regional industry recognised certifications for CSPs (e.g. ISO/IEC, NIST, IOSCO). Because the EU CCS for CSPs only references a limited number of international standards (ISO/IEC) it is unclear how the proposed scheme aligns with internationally recognised standards for CSP certification. We recommend the proposed EU CCS for CSP includes additional references to international standards as well as where alignment is achieved or is different, to provide clarity to CSPs and financial entities

using international standards. This will also support cross-border activity by enabling mutual recognition between certificates in use.

- We support efforts to acknowledge the use of internationally recognised standards and industry leading practices on information security and ICT controls. To promote consistency across the financial sector and reduce regulatory fragmentation, financial entities from various jurisdictions along with other industry associations developed in 2018 the Cyber Risk Institute's (CRI)[2] Cybersecurity Profile ("Profile"). The Profile is a globally recognised, scalable and extensible assessment tool that financial entities of all types can use for internal and external (i.e., third-party) cyber risk management and as a mechanism to evidence compliance with various regulatory frameworks, globally. We recommend EU policymakers acknowledge the Profile as an internationally recognized technical standard/industry leading practice on information security and ICT internal controls. Both the EU CCS for CSPs and the Profile are based on ISO/IEC controls for ICT security and could therefore be mutually recognised.

Section 5: Security Controls – Annexe A

- Financial entities should have flexibility in selecting an appropriate level of assurance ('basic', 'substantial' or 'high') for cloud services, even for critical activities. This would be compatible with a risk-based approach, where financial entities have flexibility in managing their risks, rather than assuming a 'high' level of assurance should be required for all critical activity. While a high level of assurance guarantees a certain level of security and control from a CSP it does not cover for all risks or consider the additional level of security provided by the financial entity. Therefore, a critical activity which has received a 'high' level of assurance by the financial entity may not always require an equal amount of assurance by the CSP.

[2] https://cyberriskinstitute.org/