POSITION PAPER

ESBG Cloud Certification Task Force
Position Paper on a Cloud Certification

ESBG (European Savings and Retail Banking Group)

Rue Marie-Thérèse, 11 - B-1000 Brussels

ESBG Transparency Register ID: 8765978796-80

June 2020

ESBG

I. Background

There is an ongoing reflection on the level of oversight and supervision for providers supplying a public Cloud to the banking and financial sectors. The underlying idea is to ensure that Cloud Services Providers deliver on a trusted European Cloud which should match with the technical, security, legal and regulatory requirements imposed by the EBA with the outsourcing Guidelines 2019 and the Guidelines on ICT and security risk management 2020 or legal acts like GDPR.

ESBG has established a dedicated Task Force for Cloud Certification as part of the work carried out in the framework of its Fintech Regulation Committee, in order to steer its work and develop a common understanding on regulatory and contractual issues when Financial Institutions are contracting with Cloud Services Providers (CSP).

Members are concerned about the unbalanced power relationship between CSP (Google, Amazon, Microsoft, Alibaba, etc) and the users of cloud services, such as banks. Members shared the view that it is almost impossible for banks to negotiate contractual terms with the powerful CSP compliant with the mentioned EBA guidelines or applicable legal acts, and that this situation generates compliance risk to Banks as they are still responsible for the outsourcing arrangement.

Regarding the regulatory framework, the EBA (European Banking Authority) in its outsourcing guidelines[1], set some obligations for banks, which can hardly be met (e.g. auditing rights, data localisation), as the negotiating position of European banks towards cloud service providers is fairly weak.

The aim of the Task Force (TF) is to build the case for an official certification scheme, with boxes that cloud service providers need to tick and requirements that they need to meet, in order for them to offer their services in the European banking market. This Position Paper intends to present some relevant criteria that cloud service providers need to meet, and it is based on the feedback that ESBG has collected from its Members.

The shared goal of the TF would be to build a standard Cloud package to provide to the banking sector (and not for each bank) that a third party officially recognised will certify. **The label or certification should assess and validate standard regulatory requirements such as technical/security/legal/compliance issues**, which are, for instance, imposed by the EBA guidelines on outsourcing.

In this position paper, the TF has identified some of the major Cloud guarantees expected from the CSP, in order to comply with the authorities' requirements, and obtain trustworthy banking Cloud services. This list could be a starting point to look at the question in more detail by authorities. ESBG will continue its engagement to reinforce and cooperate in the regulatory dialogue between public authorities and the private sector.

ESBG has gathered feedback from its Members and experts ranging from IT to Legal and data specialists. The Task Force believes that **this cloud certification would contribute to minimize technical, operational and security risks, and at the same time would contribute to the compliance of the EBA Outsourcing Guidelines. In addition it would leverage the faster adoption of new technologies in the European banking industry, to be competitive on a worldwide basis.** In any case, it appears quite clearly that a new oversight framework shall not increase the banking and financial sectors obligations and supervisions.

[1] EBA Guidelines on outsourcing arrangements, EBA/GL/2019/02

The Cloud Certification will be very useful for IaaS (Infrastructure as a Service) and PaaS (Platform as a Service). For SaaS (Software as a Service), our Members understand that it is appropriate to certify every different software application within the regulators.

II. Cloud Certification Criteria

a. Access and Audit rights

EBA Guidelines on outsourcing requires that outsourcing institutions ensure in the agreement that they have unrestricted rights of inspection, auditing and access, including for competent authorities. ESBG Members complain that it is common that banks cannot carry out audits or in the best cases, the audits banks can carry out are limited.

Members agree that it would be necessary to count on a CSP Certification to homogenize all audits in terms of frequency, content, location, cost, etc… independently of the CSP or other conditions. Ideally, this certification should be validated by the regulators to ensure compliance and to convey directly to the CSP the major requirements without putting the entire burden to Financial Institutions who most of the times don't have the ability to certify processes or to enforce requirements. Certification should be obtained in real time, in a continuous audit model.

Concrete requirements:

1) In terms of the **frequency of the audits**, Members agree that one audit on a yearly basis would be sufficient or when any substantial changes have been implemented.
2) In addition, it is important to ensure that the **CSP hand over relevant materials**, e.g. internal audit reports including action plans, to the auditors, to have an efficient and effective control.
3) The auditing of CSP should be performed across industry sectors, and requirements of other authorities like the health industry should be covered too.

b. Service Availability / Security of data systems / Business continuity

Quality, performance, security, business continuity should feed into a written outsourcing agreement and Service Level agreement and might be performed.

The performance and quality of the cloud service provider's service delivery and the level of operational risk that it may cause to the outsourcing institution or payment institution are largely determined by the ability of the CSP to appropriately protect the confidentiality, integrity and availability of data (in transit, in memory and at rest) and of the systems and processes that are used to process, transfer or store that data. Appropriate traceability mechanisms aimed at keeping records of technical and business operations are also key to detecting malicious attempts to breach the security of data and systems. Security expectations should take into account the need, on a risk-based approach, to protect the data and systems.

Concrete requirements:

1. **Security requirements**: by identifying the security risks based on a general common risk assessment and determining the necessary security controls to minimize them to a certain acceptable threshold

2. **Recognition scheme between certifications**: to avoid repeating the work all the time, so the controls validated by a certification scheme should be recognized as well as previous certifications for example in PaaS, IaaS etc.. where certifications and audits are valid. Do the CSP declare their security certification and release their security reports? Such as ISO 27001, soc 2… ISO 270xx family would be fine as a basis especially the cloud related documents like 27018 and 27019 or a security standard like BSI C5. Any kind of certification has to be directly related to the full scope of the provided services.

3. **Commitment that access of CSP or its subcontractors to customer systems and data requires customer approval prior to the access.** Technical implementation must ensure that all accesses to customer systems and data need to be tamper-proof, recorded, and accessible by customers at all times e.g. session recording of the administrator session. If an access will be performed without the customer's approval e.g. in case of emergency or due to legal issues like CLOUD-ACT, the customer has to be informed immediately in detail (who, when, why, what data are accessed) by the CSP.

4. **Commitment to continuously improve security implementations, processes and procedures to reflect state-of-the art implementations, not to change unilaterally the terms and conditions by the CSP and the obligation to inform.** Terms and conditions should be changed on a regular basis only e.g. twice a year and should be approved e.g. by a joint customer board or a legal authority.

5. **Commitment to obtain information related to security breaches, and a formal process to solve problems and incidents.** ESBG supports full visibility and transparency to all customer related issues like security breaches, identified risks, audit findings etc.

6. **Commitment to obtain a clear responsibility of CSP in case of any performance or quality issues:** Clear European-wide uniform Service Level Agreements must be defined and measured by the CSP. The methodology for calculating those fulfilments need to be defined.

7. Based on these common standards **a European-wide minimum security standard** (policies and procedures) should be developed by a legal authority based on international standards like ISO 27xxx or ISAE 3402 and European best practices like the German BSI C5 or the French Cloud NumSec. CSPs should publish the internal security policies at least on a yearly basis and the KPIs regarding achievement at least on a quarterly basis.

8. **Obligation of the CSP to release their security certification of the defined security standard**, including the certification report, e.g. SOC2 and all relevant documentation like the recommendations/findings, plus the action plan and status for closing them

c. <u>Data</u>

ESBG agrees that data should be handled with special care when entering into outsourcing agreements outside EEA and is fully committed to complying with GDPR requirements. According to EBA outsourcing guidelines, Banks should adopt a risk-based approach to data and data processing location considerations.

CSP shall give the location for processing and storing customer data, which shall be mentioned in the contract.

ESBG is fully committed to GDPR compliance.

Concrete requirements:

1. **Indication of the location of data storage and data processing**: the EBA guidelines and GDPR require focus on data processing; this includes data in rest and data in motion. We need a comprehensive overview per service where data is processed as a requisite.
2. **Applicable law of the contract in a European jurisdiction**: this will reinforce the interests of outsourcing institutions and compliance with the European regulatory framework. Further reflection will help to homogenize criteria, because nowadays regulation benefits non-European companies, and sometimes it is necessary to evaluate more accurately the balance between security of data and business & user experience, to adapt protection of data to the real necessities.
3. **Commitment to authorized people or users to have access to the data.**
4. **Commitment that each data access by the CSP or its subcontractors to customer data is acknowledged to the customer** without additional service cost (who, when, why, what data are accessed)
5. **Commitment that access of the CSP or its subcontractors to customer systems and data requires customer approval prior to the access.** Technical implementation must ensure that all accesses to customer systems and data need to be tamper-proof, recorded and accessible by the customer at all times, e.g. session recording of the administrator session. If an access will be performed without customer approval e.g. in case of emergency or due to legal issues like CLOUD-ACT, customer has to be informed immediately in detail (who, when, why, what data are accessed) by the CSP.
6. **Commitment concerning the data location (customer and meta data)**: Data location can be completely configured by the customer and it is a general policy to exclude specific regions (e.g. the US) from data location and processing. A European Certification Scheme for CSP could ensure that data is in the European space and strictly following the European legislation.
7. Clarification on what is the **use of the metadata and other information that could be inferred indirectly from the data.**
8. **Data Classification is the sole right of the bank, and the CSP has to strictly adhere to it whenever any kind of bank data is concerned.**

d. Chain outsourcing

Obligation for the CSP to notify the outsourcing institution of any planned significant changes to the sub-contractor named in the contract, which might affect the cloud service provider.

The outsourcing institution should agree to chain outsourcing only if the subcontractor will fully comply with the obligations between the outsourcing institutions and the CSP.

Information concerning sub-contractors must be provided and updated.

1. **Require a pre-notification from CSP**: that should follow the same rules as any other outsourcing, in most of the cases the CSP have outsourced everything beforehand.
2. **Commitment from the CSP that its contractual relationship with a sub-contractor comply with your requirements**: Most of the times, but in the case they don't do it responsibly it should be assigned to CSP's
3. Full information related to the subcontractors from the CSP: a full overview of the outsourcing chain is required. Clear guidelines are needed for the involvement of a subcontractor.

e. Contingency plans and exit strategies

The outsourcing contract should be an obligation of the CSP to sufficiently support the outsourcing institution in the orderly transfer of the activity to another service provider, or to direct management of the outsourcing in the event of a termination.

Exit strategies arrangements from cloud outsourcing shall be without undue disruption to its provision of service and without detriment to the continuity and quality of its provision of services to the client.

Concrete requirements:

1. Commitment that the CSP will undertake reasonable efforts to support the migration process and the data deletion after the migration.
2. Commitment that the CSP will provide services based on open standards to ensure interoperability and portability between other market participants in the cloud service.
3. The CSP should undertake reasonable efforts to meet service requirements (SLA) and to optimize the service in case of failure in a defined timeframe.
4. In case of a contract termination an active exit support has to be provided by the CSP. All customer data has to be handed back by the CSP and deleted securely afterwards upon customer approval. If the data is stored in a proprietary data format, a conversion to an open data exchange standard must be possible and provided by the CSP.

III. Conclusion

The EBA has advised the European Commission to look at the establishment of **an appropriate oversight framework for third party service providers (TPPs), in particular in the area of cloud services.**

ESBG encourages and shares the need to strengthen and harmonise the current legislative framework for TPPs in two ways: micro and macro.

- **At the micro level**, we need to strengthen the toolkit to enable supervisors to supervise more effectively the activities, which are provided by third parties. Such strengthening should enable supervisors to have access rights, audit rights and sanctioning rights directly from the regulatory framework rather than relying only on contractual provisions in outsourcing contracts. **ESBG believes that the Cloud Certification is an additional toolkit and will contribute to achieve this policy objective. ESBG encourages policy makers to increase policy efforts to create a CSP certification framework.**

- **At the macro level**, ESBG also agrees with the EBA that for critical TPPs, there is an urgent need for a new oversight framework that sets higher standards related to security and data protection (e.g. obligatory cybersecurity certification). The scope of oversight should aim at monitoring concentration risk, financial stability risks, and ensuring cooperation with relevant authorities.

ESBG welcomes the European Commission's approach to standardizing certain mandatory and sensitive Cloud contractual clauses. Nevertheless, it should go in parallel with additional efforts to strengthen financial sector capacity to negotiate. Beyond the standardization of Cloud contractual clauses, a complementary approach could be considered to obtain a Trustworthy European Cloud for the financial

sector, with the creation of a label relating to Cloud categories (to be defined) and according to their criticality as an essential service.

ESBG and its Task Force believes to have built the case in a consistent manner for all European Authorities to implement this label or certification that should include a holistic list of criteria of legal, technical and security requirements (e.g. derived from the EBA guidelines 2019). The providers would be forced accordingly to adopt this label to the Cloud service «by design » for the banking and financial sector. The compliance with these guidelines should be centrally controlled by a legal authority to guarantee a European-wide uniform verification and to minimize individual effort for each customer.

About ESBG (European Savings and Retail Banking Group)

ESBG represents the locally focused European banking sector, helping savings and retail banks in 21 European countries strengthen their unique approach that focuses on providing service to local communities and boosting SMEs. An advocate for a proportionate approach to banking rules, ESBG unites at EU level some 900 banks, which together employ more than 650,000 people driven to innovate at roughly 50,000 outlets. ESBG members have total assets of €5.3 trillion, provide €1 trillion in corporate loans (including to SMEs), and serve 150 million Europeans seeking retail banking services. ESBG members are committed to further unleash the promise of sustainable, responsible 21st century banking. Our transparency ID is 8765978796-80.

European Savings and Retail Banking Group – aisbl
Rue Marie-Thérèse, 11 ■ B-1000 Brussels ■ Tel: +32 2 211 11 11 ■ Fax: +32 2 211 11 99
Info@wsbi-esbg.org ■ www.wsbi-esbg.org

Published by ESBG June 2020.