Draft recommendations on outsourcing to cloud service providers under Article 16 of Regulation (EU) No 1093/20101

SPA Position on EBA Consultation

Summer 2017

1. Are the provisions from these recommendations clear and sufficiently detailed to be used in the context of cloud outsourcing?

SPA considers that these recommendations are welcome to complete the CEBS guidelines when outsourcing financial services to the very specific Cloud computing environment. Cloud is here to stay and as its use generalizes, cloud computing facilities will be subject to more security threats (cyberattacks, data theft, data disclosure) as well as to technical incidents compromising services. These threats have to be mitigated with effective countermeasures. With this regard, we believe that

1. a more detailed level of security & privacy requirements and
2. being more precise with regards the responsibility for the implementation of security controls would help to fix liability in outsourcing contracts.

On the other hand, in that case, this draft would be more prescriptive than the existing CEBS guidelines, creating a consistency issue. As for any legal text a trade-off is to be found and this text represents an acceptable compromise for existing market players. However the risk is that by remaining "high-level" these guidelines merely reflect "state of the art practices", already applied by Cloud Service Providers and the financial institutions.

Meaning a very limited impact in the industry and not really contributing to:

1. improving the customer protection lack of promoting common risk management policies when outsourcing core processes to cloud service providers
2. promoting high-quality financial services if the use of cloud redundant technical infrastructures robust enough to ensure business continuity is not prescribed
3. incentive competition among cloud financial service providers, necessary to avoid early commoditization of cloud-based financial solutions. Competition must be organized on the grounds of common good practices.

That's recognized in the end of clause 5D ("since most of the institutions currently have similar procedures in place the marginal cost of implementing these supervisory changes is expected to be small or negligible").

2. Are there any additional areas which should be covered by these recommendations in order to achieve convergence of practices in the context of cloud outsourcing?

In our opinion, the convergence of practices also relies on the common understanding of the legal financial compliance landscape. The legal texts and recommendations constitute at present "bricks" with insufficient mortar. Recommendations may or not be followed by a financial institution, made mandatory or not in a particular member state, and that creates uncertainties and adds complexity for technology vendors and also for Cloud Service Providers. Recommendations are welcomed and provide useful guidance and a level of flexibility for innovation, yet they should constitute a first step.

These recommendations address five main areas relevant for financial institutions outsourcing cloud computing services:

- Guarantee access and audit rights, for the cloud outsourcing institutions and the national financial supervisors
- Controls for chain cloud outsourcing
- Business continuity & contingency plans
- Location of data and data processing with a focus on privacy aspects
- Security of Cloud-stored data and systems

Because of the business activities of SPA members, we feel more comfortable commenting on the security aspects of Cloud Outsourcing.

General Comment

SPA notes that the specific security countermeasures to be contractually required to mitigate specific vulnerabilities of Cloud are not addressed. Clauses 4.5 and 4.6 are generic high-level "common-sense" recommendations that apply to any contractual arrangement with a technical service provider (Cloud or not) managing sensitive data. Clause 5.D notes that "instead of providing specific guidance… ,the EBA prefers to introduce as much as possible technology-neutral…". But Cloud is about technology (a new computing model sustaining a new business model) to store, execute and manage data and applications. In the Cloud, financial customer data is outside its control and could potentially be granted to untrusted parties. This model adds specific vulnerabilities that cannot be ignored in an outsourcing contract and whose control should be reflected in more specific practices in this document (they can be references to existing relevant materials released by recognized organizations).

Recommendations such as "define and decide upon an appropriate level of protection of data" or "institution should also consider specific measures where necessary such as the usage of encryption with appropriate key management architecture" are of course fine but don't contribute to harmonize cloud security engineering practices.

It can be argued that this is the role of technical standard bodies, such as ISO JTC1 SC38 or the European Cards Stakeholders Group (ECSG) for card payments using the Cloud. But then cross-references in this document to such standards or other relevant EBA Regulatory Technical Standards are needed. For instance Key Management Systems are always in scope of PCI audit, even if how to apply PCI Key Management requirements to the Cloud context is challenging.

To complete these draft guidelines, SPA proposes the following:

1. Include recommendations for outsourcing Mobile Cloud Computing
2. Include recommendations/requirements for customer Cloud segmentation
3. Include references to standards and regulations that can be contractually required, including standard security certification practices and

To complement these draft guidelines, SPA proposes the following:

4. Elaborate a Risk Management Guide for Financial Cloud-based Services
5. Produce a kind of "Common Security Best Practices for Financial Cloud-based services"
6. An assessment guide for the security of Financial Cloud Service Providers

2.1. Include provisions for Mobile Cloud Computing

General remark

Most of the commercial Cloud based solutions are now one-click solutions that could be also accessed via a consumer mobile device. Mobile Cloud Computing has a longer processing chain involving more players (eg, OEM, Mobile Network Operators). More intermediaries means additional vulnerabilities and more investment in security to be shared/coordinated to ensure safe cloud usage. With this respect we believe that adding specific guidelines for Mobile Cloud computing could be beneficial.

To start with, we suggest a new definition to be added in Ch2:

"Mobile Cloud Computing": Combination of mobile network functionality and cloud computing allowing customer applications to be executed and data to be stored in a cloud facility (i.e., internet servers) using a mobile device.

- Outsourcing Mobile Payment Services to Cloud Providers

SPA members are technology vendors in the payment card industry. The combined use of Cloud and mobile payment technology is mainstream. New technical architectures for mobile contactless payments combine the use of local and remote storage and computing facilities for personal payment and authentication credentials. Theses credentials are issued by banks during the customer enrollment and stored in a cloud computing database. The compromise of such a database could have serious consequences. New cloud computing accounts may be opened with stolen card payment credentials anonymizing the criminal and making tracking down difficult when several jurisdictions are involved.

Setting out more detailed contractual requirements to protect access to outsourced Cloud payment credentials and other personal data could have an interest to harmonize implementations. In this context the use of specific technical standards and certification processes could be recommended (see below).

2.2. Include recommendations/requirements for customer Cloud segmentation

In clause 3 of the document, the EBA notes that, compared with traditional outsourcing models with a highly-profiled client-solution, cloud outsourcing services are managed to serve a larger number of different customers and to a much larger scale to benefit from economies of scale. Better security is achieved by not mixing in the same computing environment trusted (payments) and untrusted financial applications. Financial data are valuable for criminals and security computing resources specific to protect them are to be assigned to them. PCI-DSS, specific to card payment data, recommends the segmentation by the Cloud Service Providers of cloud applications that process payments from non-payment applications. With this regard, isolation of financial data should be contractually guaranteed as well.

2.3. Include references to standards and regulations in outsourcing contracts

This point has been previously evoked. Between legal texts or recommendations provided by the EBA and concrete technical implementations by vendors of cloud-based solutions, there's a gap. For the purpose of outsourcing contracts for financial services, different standards both technical and regulatory are relevant references.

Thus, with respect to vocabulary, architecture and data flows using connected devices, the following ISO standards could be referenced

- ISO/IEC 17788 is the first attempt to standardize cloud-related terminology and the SPA recommends to align vocabulary with this standard
- ISO/IEC 17789 provides with a reference architecture for Cloud Computing
- ISO 19994 by ISO JTC1 SC38, completes the above materials to describe an ecosystem involving devices using cloud services on Cloud services and devices: Data flow, data categories and data use. It's a cross-industry descriptive not prescriptive standard, that anyway provides with

Thus, with respect to cloud security and privacy

- The EBA RTS on Strong Customer Authentication (when available) should be referenced to (1) mandate authentication practices for access to Cloud-based payment services and (2) Chapter 4 refers to the requirements for the confidentiality and integrity of the payment service users' personalized security credentials.
- PCI-SSC has released specific guidelines for the application of PCI-DSS to Cloud Computing environments. PCI-DSS only applies to card payment data protection and is not necessary

relevant for other types of payment services. Yet PCI-DSS has no legal status, and compliance can only be enforced by contract

- The Cloud Security Alliance (CSA), the world's leading organization dedicated to defining best practices for a secure cloud computing environment, has initiated a collaboration with ISO/IEC JTC 1/SC 27.

With respect to Service Level Agreement contractual requirements

- ISO 19086-1 provides with useful material to contractually fix Cloud Service Level Agreement requirements in a harmonized way.
  - With that respect, to protect the customer, it's suggested that the financial institution contractually requires from the Cloud Service Provider evidence proving the integrity and the availability of customer stored data at any time.

2.4. Elaborate a Risk Management Guide for Financial Cloud-based Services

SPA considers that a common understanding by financial institutions of the structure of risk when outsourcing financial services to the Cloud could help better negotiate contractual provisions with Cloud Service providers.

The Basel Committee on Banking Supervision (BIS) proposed Risk Management Principles for Electronic Banking in 2003. In the report the BIS introduced 14 principles which were broadly divided into three categories namely: Board and Management Oversight (Principles 1 to 3), Security Controls (Principles 4 to 10) and Legal and Reputational Risk Management (Principles 11 to 14). These principles were produced before the Cloud Computing Model was created. However, this document could be profiled to elaborate a Risk management guideline specific for Cloud outsourcing.

In the EEA, we notice the existence of ENISA's document "Secure Use of Cloud Computing in the Finance Sector". However this document is an assessment (Dec 15) of the level of Cloud Computing uptake technology by financial institutions, of their concerns and expectancies and not a risk management guide.

2.5. Produce a document of "Security Recommendations and Best Practices for Financial Cloud-based services"

IT security is difficult under all circumstances and the way Cloud computing operates data and application makes things more complex. As an example, there is a controversy in the industry with regards the real applicability of the PCI-DSS profile for Cloud Computing payments. Certification then against PCI-DSS may become complex for the Cloud Service Provider.

The loss of control of data by the financial institution is a risk. Moving customer data to the Cloud means that the Cloud Service Provider (or a third party subcontracted by the Cloud Service Provider) is controlling these data. Yet for small companies (eg Fintech) Cloud providers are likely to have better security than them, but overregulated financial institutions are not necessary to benefit from the security expertise at the Cloud provider. In any case, both worlds have a strong incentive to have good contracts with Cloud Providers in terms of security.

The functional requirements at the core of the Cloud Computing model bring about security concerns specific to the Cloud, for which specific adapted cryptographic mechanisms have been designed but not sufficiently proven by the financial industry (homomorphic encryption , group signature).

In any case, the direct access to encrypted data in the Cloud by the owner himself of by an authorized third person, raises specific challenges in terms of key management. As a minimum, Cloud sensitive data must be encrypted in transit and the keys required to decrypt the content must be made available to the final user of the data. Because of the variety of possible implementation scenarios the key management system in the Cloud is necessary complex to achieve. Because of this complexity, it will be expensive to implement and operate.

According to these draft guidelines (Clause 4.5) proper monitoring and audit of the Cloud Service Provider practices for the security management of keys should be required. In the important scenario for SPA of card payments, the PCI-DSS requirements for key management appear difficult to apply by Cloud Service Provider implementations. Further guidance could be useful.

The industry highly appreciated the publication by the SecurePay of the recommendations for the security of Internet Payments. A similar document could serve as a common basis for the financial institutions contractual provisions in terms of the security of financial Cloud infrastructures.

This document could be the opportunity of a collaborative work between the EBA and the payments industry, providing technical expertise.

2.6. An assessment guide for the security of Financial Cloud Service Providers

This deliverable could help outsourcing financial institutions as well as supervisory authority officers of members states to assess compliance with the recommendations set out in the previous document during their auditing duties as per clause 4.3.