How IBM supports banks in the context of European Banking Authority recommendations on Cloud Computing

IBM **Cloud**

IBM

Introduction

European Banking Authority (EBA) issued the '*Final report on recommendations on Cloud Services Providers*', applicable as of July 1st 2018 to provide additional guidance to EU credit institutions and investment firms (generally known as Financial Institutions, or FIs) around the 'Committee of European Banking Supervisors guidelines on outsourcing' (CEBS guidelines) on outsourcing to Cloud Service Providers (CSP).

In addition to the former CEBS guidelines, the EBA recommendations focus on six main areas for EU Financial Institutions:

1. Assess materiality of cloud outsourcing and Information of regulators
2. Right to access and right to audit for institutions and competent authorities
3. Security of the data and systems used
4. Location of data processing
5. Chain outsourcing
6. Contingency plans and exit strategies

IBM welcomed the European Banking Authority's initiative and actively participated in the consultation process with the goal of setting a common regulatory framework for outsourcing to Cloud Service Providers for the benefit of all parties. IBM believes that the EBA's recommendations will benefit and support the adoption of cloud and enable further convergence of both Financial Institutions and supervisory practices and expectations.

IBM is deeply committed to support FIs in addressing the challenges of cloud outsourcing.

Our global financial services industry expertise, together with our global experience on outsourcing gives IBM a deep understanding and wide perspective of Financial Institutions' needs and requirements. We have taken those requirements to our cloud platform and can offer unparalleled capabilities for core and peripheral workloads.

These capabilities are complemented by our contractual framework, covering the specific focus areas highlighted by the EBA recommendations and enabling Financial Institutions to get the benefits of cloud while addressing their business controls and applicable regulations.

In summary, IBM Cloud provides an environment capable of allowing outsourcing institutions to comply with the EBA recommendations on cloud outsourcing when using IBM Cloud for both material and non-material activities.

IBM addresses Cloud Services Providers Requirements

Financial Institutions are currently under a lot of pressure to address customer and stakeholder expectations, while complying with increasing regulatory requirements. IBM leverages its deep industry expertise to design, deliver and continuously upgrade its cloud environment to address financial services industry requirements, including the EBA's recommendations on outsourcing to CSPs. IBM as CSP addresses its obligations as follows.

Materiality of cloud outsourcing, to inform competent authority

Following CEBS guidelines, the EBA requires outsourcing institutions to assess materiality of activities and inform the competent authorities, in addition to a requirement that outsourcing institutions maintain a register of both material and non-material outsourced activities.

Although the performance of a materiality assessment and subsequent informing supervisors remains the responsibility of the outsourcing institution, IBM can help to support the requirements necessary to help FIs achieve their business targets and successfully meet their regulatory posture. Each IBM Cloud service has a clearly outlined Service Description that distinctly articulates the details of that service in support of the requirements of materiality assessment. IBM can help to assist firms in assessing and documenting the materiality of activities and outsourcing information to be sent to the EBA.

Right to audit for institutions and competent authorities

As required by the EBA and CEBS guidelines, outsourcing institutions and competent authorities should ensure they have full access to the CSP business premises, unrestricted rights of inspection and audit related to the outsourced services.

The list of the EBA recommendations supports IBM's approach to the use of independent third-party globally recognized and accepted certifications and reports as a proportionate and risk-based approach to address due diligence and subsequent ongoing monitoring. IBM maintains a comprehensive list of compliance certifications and audit reports. A full list is available from the IBM Cloud Compliance web page where instructions to obtain copies of specific reports can be found.

IBM Cloud is designed and built for critical and non-critical workloads from a security and resiliency perspective, as proven by our *certifications* and the confidence of Financial Institutions: both global and European Financial Institutions have selected IBM to help drive innovation at process and infrastructure technology levels, outsourcing both material and non-material activities to IBM Cloud.

IBM has developed a Cloud Addendum for Financial Services Sector, with contractual obligations including providing audit and access rights for its clients aligned with the EBA recommendations.

IBM has, since 2016, a Cloud Compliance Advisory Body (CCAB) for Financial Institutions. This board meets, on a quarterly basis, to address issues and concerns of individual and global regulatory requirements. Participation in the CCAB also provides insight into IBM's internal controls assessments process, further expanding on the coverage provided through extensive external certifications and audit reports.

Security of data and systems

The EBA recommends that outsourcing institutions classify the activities to be deployed to the Cloud Services Provider, to determine an appropriate level of: protection of data confidentiality, continuity of activities outsourced, and integrity and traceability of data and systems in the context of the intended cloud outsourcing.

IBM Cloud provides Financial Institutions with unique capabilities in terms of security for data and systems, providing the capability to host the most demanding workloads. The *Data Security and Privacy Principles for IBM Cloud Services* document describes the security principles driving the technical and organizational measures implemented for all IBM Cloud Services. Specific technical and organizational measures deployed by IBM for each IBM Cloud Services product are described within the *Cloud Services Data Sheets*.

From environment isolation to data encryption and even dedicated physical infrastructure, Financial Institutions can choose from a wide variety of security options to deploy their workloads, depending on their specific requirements.

If additional security capabilities are required, IBM can work with the Financial Institution to offer additional security solutions to meet any enhanced requirements for the Cloud environment.

Locations of data and data processing

Outsourcing institutions should take special care when entering outsourcing agreements undertaken outside the EEA because of possible data protection risks. The EBA recommends outsourcing institutions adopt a risk-based approach to data and data processing locations, including legal risks and compliance issues.

IBM Cloud Services are available and hosted from a variety of locations (the complete list is available here), allowing Financial Institutions to select their preferred deployment location for an IBM Cloud Service, knowing that their Cloud Service and data will remain within the selected location.

For every IBM Cloud Service, a specific Data Sheet is made available with detailed IBM hosting and processing locations. The Data Sheets repository can be reached here, issued in support of overall data privacy requirements and supported by IBM's Data Processing Addendum. In the event that part of an IBM Cloud Service is provided outside the EEA, IBM enables customers use of the *European Union Model Clauses (EUMC)*, making sure IBM Data Importers have adequate safeguards in place with respect to the protection of privacy and fundamental rights and freedoms of individuals. Further, IBM is a member of the European Cloud Code of Conduct general assembly.

Chain outsourcing

Institutions should take into account the risks associated with 'chain' outsourcing: consistency of obligations along the subcontractors' chain must be granted, prompt notification must be issued when significant changes in subcontractors' chain are planned, and clear responsibilities under the outsourcing agreement must be attributed.

As required by CEBS and reinforced by the EBA recommendations, any third party used by IBM to provide Cloud Services in IBM Cloud Data Centers will follow the same obligations agreed between IBM and the Financial Institution. Moreover, IBM will require subprocessors, with access to customer content, to maintain technical and organizational security measures that will enable IBM to meet its obligations for a Cloud Service. A current list of subprocessors and their roles will be provided upon request. Institutions can check the list of third-party sub processors (if any) for IBM Cloud Services in each service's Data Sheet.

Important to notice is that IBM will contractually agree with the Financial Institution a notification period for changes in Subcontractors chain, to enable the customer to complete its internal risk assessment.

Contingency plan and exit strategies

The EBA recommends outsourcing institutions plan and implement arrangements to maintain the continuity of its business and include a termination and exit management clause. The Cloud Services Provider has to support the transfer of the activity to another service provider or to the direct management of the outsourcing institution in the event of the termination of the agreement.

IBM Cloud defines a business continuity plan per IBM Cloud Service, as defined in the *Data Security and Privacy Principles for IBM Cloud Services*. Moreover, business continuity plans for each service are provided as part of IBM Cloud Service Data Sheet.

IBM Cloud Services Agreement includes the option to exit an IBM Cloud Service if for legal reasons the Financial Institution cannot accept changes to an IBM Cloud Service. Further, the Cloud Addendum for Financial Services addresses the EBA requirement for the CSP to support an outsourcing institution in the transfer to another services provider.

Summary

Financial Institutions can use IBM Cloud to deploy material outsourcing activities. IBM Cloud addresses FIs EBA requirements on outsourcing to Cloud Services Providers. IBM's industry expertise, combined with our Cloud capabilities, can provide Financial Institutions with benefits in cost, agility and speed, keeping control on the outsourced activities, as requested by the EBA. IBM can support Financial Institutions on every step of their journey to cloud, from design to migration, using Cloud Services prepared for highly regulated workloads.

Disclaimers

Customers are responsible for ensuring their own compliance with various laws and regulations. Customers are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the customers' business and any actions the customers may need to take to comply with such laws and regulations. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that customers are in compliance with any law or regulation. Although every attempt was made to ensure the accuracy of this document, the information presented herein may be incomplete or inaccurate and no representation or warranty of any kind is made as to its accuracy, reliability or completeness.

Useful Link:

www.ibm.com/cloud/banking/security

Prepared by:

Nicolò Lorenzoni
IBM Cloud Architect Leader FSS

Giovanni Boniardi
Senior Infrastructure Consultant

Luis Lara Pezzi
Cloud Platform FSS Industry Lead for Europe

Reviewed by:

Heather Hinton
Hybrid Cloud CISO

David Cass
Cloud and SaaS CISO

Carlo Comporti
Promontory Financial Group - Managing Director

Mafalda Garcia
Counsel

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
October 2018