



**MLADVISORY**  
RISK AND FINANCE, TOGETHER

*Assessing Outsourcing Opportunities and Challenges Associated  
with Regulatory Reporting Processes*

**12th of June 2019**

# Agenda





## DEFINITION AND PERIMETER

### *Definition*

- EBA released in February 2019, the final report on “Outsourcing arrangements”
- The definition of outsourcing is based on Commission Delegated Regulation (EU) 2017/565 and in line with MiFID. Assessment to whether the service provided should be considered as outsourcing or not should be based on:

“whether the function (or part thereof) that is outsourced to a service provider is **performed on a recurrent or an ongoing basis** and whether this function (or part thereof) **would normally** fall within the scope of functions **that would or could realistically be performed** by institutions or payment institutions, **even if the institution or payment institution has not performed this function in the past.** “

- A lot of comments have been made by respondents to the consultation paper in relation with the lack of precision of the definition. EBA has adjusted the definition by:
  - Adding “On-going or recurrent” to clarify outsourcing from purchasing
  - Adding “Realistically” and by extending the list of basic exclusions
- No distinction is made between **internal outsourcing** and **external outsourcing**
  - Banks are requesting to have lower obligation for intra group (internal outsourcing)
- Distinction is made between **outsourcing to a Member State** and **outsourcing to third countries**
  - Additional requirements for third countries
- Distinction is made for “**critical or important**” activities



## DEFINITION AND PERIMETER

### *Perimeter applied to Regulatory Production*

When applied to regulatory production, outsourcing can bring several benefits depending on the tasks that are considered

- **Regulatory watch :**

- The regulatory environment has become very complex and is under permanent changes.
- Being sure to monitor properly, within the expected deadlines, and to understand all the impacts for the institution is getting very challenging.



**Security and Professionalism**

- **Production workforce :**

- The regulatory production has increased a lot in complexity and sensitivity and is needing an increasing number of trained professional.
- Finding adequate resources is a challenge for all the institutions and ensuring good career path for the individuals is not easy.



**Save cost, ensure resilience and professionalism**

- **Information System :**

- Banks invest significantly in order to adjust legacy systems to the new regulatory paradigm
- Reporting tools doesn't bring any competitive advantage



**Save cost** by mutualizing part of the IT developments

- **Cloud computing :**

- Banks are facing an increasing need for computation capacities (higher granularity, and frequency)
- The cost needed for traditional computation in order to accommodate the increasing need is getting very high



**Save cost while reaching better performances**



## OPPORTUNITIES

### *Objectives of Outsourcing*

#### 4 main objectives :

- **Cost reduction : 3 levers**
  - Offshoring to third countries with lower employment salary and lower facility costs
  - Reduction of IS costs linked to reporting or computing capacities
  - Mutualisation of tasks with others clients
- **Quality and expertise :**
  - Dedicated teams with focused expertise vs multi tasks teams for small banks
  - Client Service Agreement ensuring formalized guidelines and expectations
  - Mutualisation of knowledge with other clients
- **Resilience :**
  - Split of risk between different locations
  - Critical size teams allowing human resources risks decrease (back-ups, more people to spread the work)
- **Access to new technology :**
  - Cloud computing, Reg Tech, etc.
  - More agility



## MAIN CHALLENGES

### *Operational challenges – How to scope the perimeter ?*

#### **The perimeter view**

Ensuring consistency between reportings that are outsourced and the ones that are not is a challenge :

- Inter-reporting controls
- Data quality corrections should be done upstream
- Governance to review figures

#### **The process view**

Regulatory reporting is the last tasks of a complex process.

Outsourcing can then start at different stages :

- Data quality monitoring and corrections,
- Calculation phase,
- Reporting phase only.

#### **The system view**

Outsourcing is driven by the information system view :

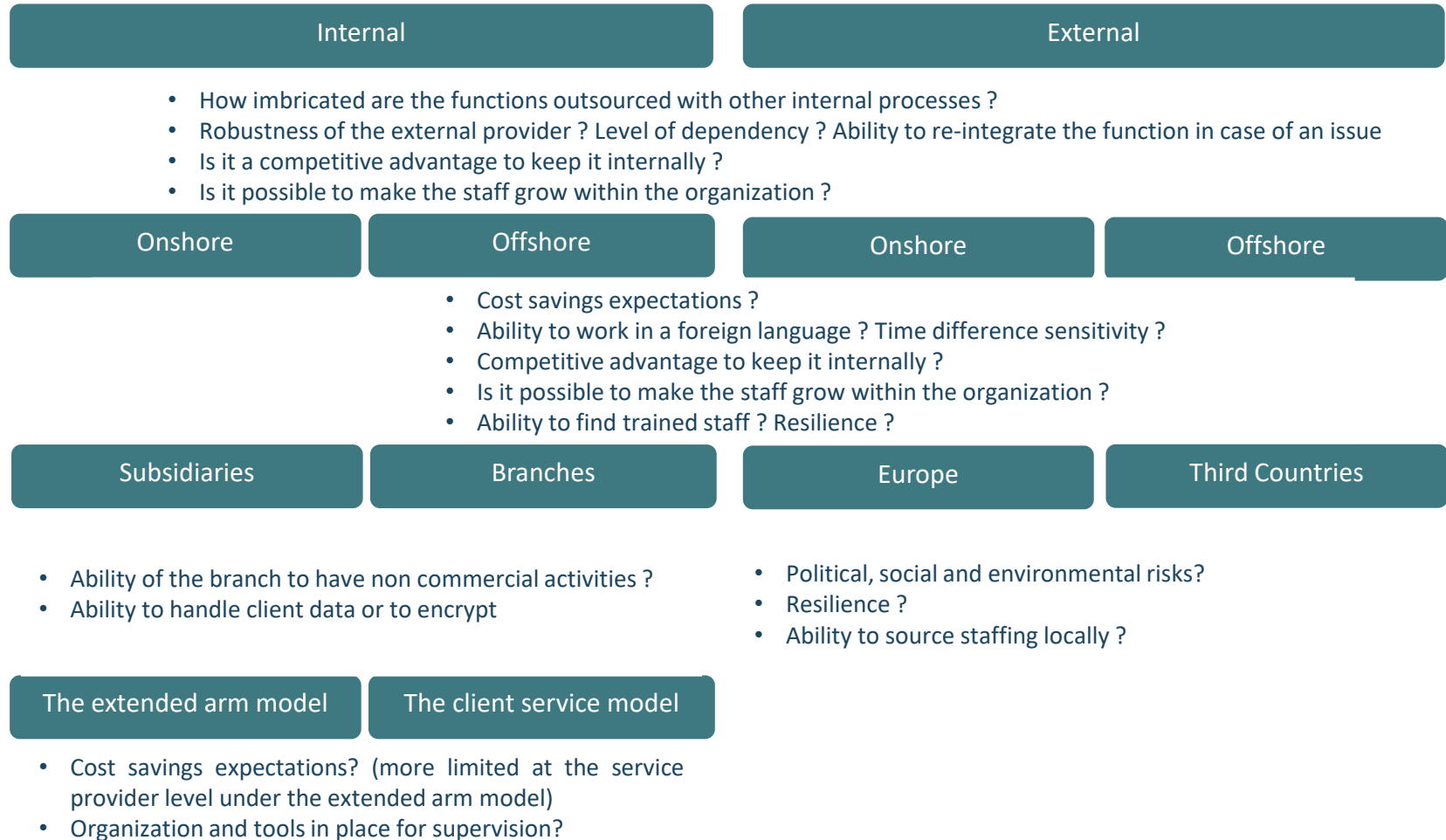
- Use of the internal system for all the production
- Partial use of the internal system
- Use of an external provider system



## MAIN CHALLENGES

### *Operational challenges – what kind of outsourcing ?*

- **Different factors to consider for the outsourcing model**





## MAIN CHALLENGES

### *Operational challenges – How to supervise ?*

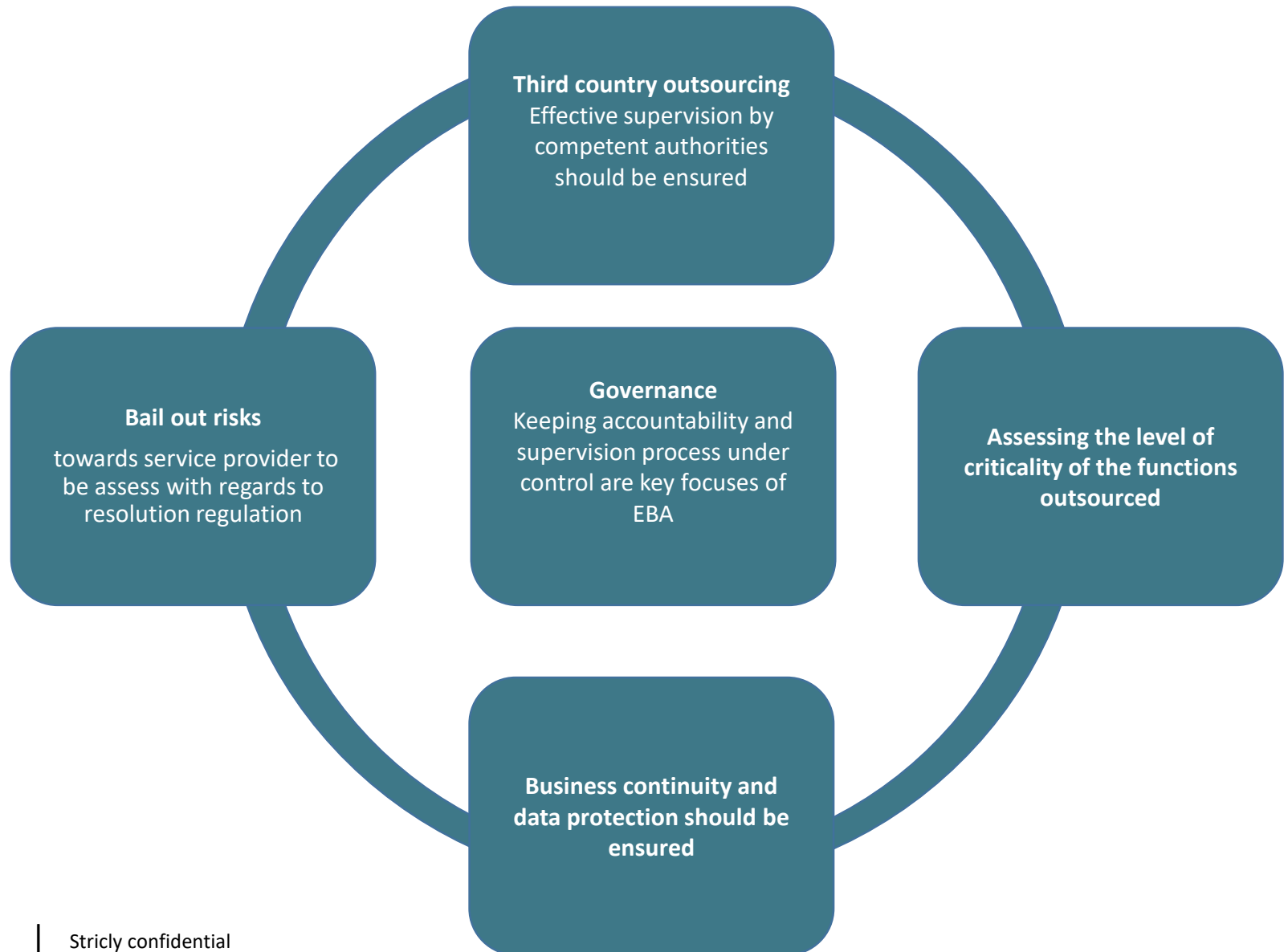
- One major driver: the **accountability remains with the entity that is outsourcing** its production
- The entity that is outsourcing its production has to **implement the tools in order to remain accountable** : certification package, internal audit review, additional analysis
- The entity that is outsourcing has to get a **global view of the risks** including the ones taken by the service provider and resulting from the use of a service provider (resolution more complex, resilience, data confidentiality, etc.)
- For external or internal outsourcing, it **should be formalized through a SA contract**





## MAIN CHALLENGES

### *Regulatory challenges*





## MAIN CHALLENGES

### *Regulatory challenges*

- **Data protection and banking secrecy around client data (GDPR, Banking Secrecy, MiFid, cloud outsourcing) :**

- **The protection of client data** has been reinforced significantly through GDPR regulation,
- **The use of client data** outside the institution managing the client is highly regulated,
- **Even within the same Group**, subsidiaries cannot have access to other subsidiaries client data without respecting the regulation limitation :

**As an example** if a Group wants to outsource activities involving client data to one of its subsidiary it has to go through the processes related to each country's banking secrecy regulation (information to client, written approval from client, etc),

⇒ **Data encryption** seems to be a solution to respect all the regulations around data protection whether it is for internal or for external outsourcing.



## Organizational Risks

Lock-in

Loss of Governance

Compliance challenges

Loss of business reputation  
due to cotenant activities

Cloud service termination or  
failure

Cloud provider acquisition

Supply chain failure

Changing regulations

Insufficient skills and  
knowledge to identify risk  
related to Outsourcing/Cloud  
computing

## Technical Risks

Resource exhaustion; under or  
over provisioning under or over  
provisioning

Isolation failure

Cloud provider malicious insider  
– abuse of high privilege roles

Management interface  
compromise

Intercepting data in transit

Insecure or ineffective deletion  
of data

EDOS

Data leakage on up/download,  
intra-cloud

DDOS

Loss of encryption keys

Undertaking of malicious  
probes or scans

Compromise service engine

Conflicts between customer  
hardening procedures and  
cloud provider

## Compliance Risks

Right to audit for supervisors

Subpoena and e-Discovery

Where is the data

Risks from changes of  
jurisdiction

Data protection risks

Specific local data privacy

Risks of conflicting regulations

Exit clause in contract

Licensing risks

## Other not Cloud Specific Risks

Network breaks

Network management

Modifying network traffic

Privilege escalation

Social engineering attacks

Loss of compromise of  
operational logs

Loss of compromise of security  
logs

Backups lost, stolen

Unauthorized access to  
premises

Theft of computer equipment

Natural disasters

Conflict of interest

Bandwidth limitations



#### **Disclaimer**

The information contained here is of a general nature and is not intended to reflect the characteristics of a particular institution.

Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future.