Cloud outsourcing in Financial Services

February 2021

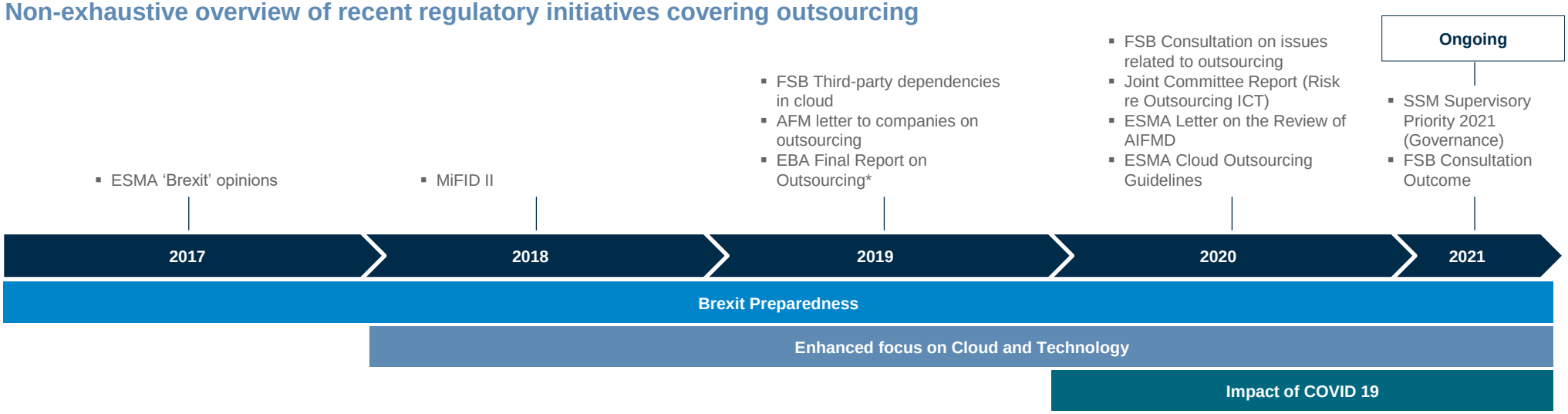
ALVAREZ & MARSAL
LEADERSHIP. ACTION. RESULTS.SM

Assessing the ESMA guidelines

Contextualising cloud outsourcing in Financial Services

- Financial institutions frequently outsource aspects of their operations, either to other group companies or independent third parties. Among other reasons, this is motivated by:
  - Cost effectiveness of using external resources;
  - Skills, expertise and/or technology offered by the external party; and
  - Firm's strategy in relation to allocation of internal resources.
- The extent and nature of interactions with third parties has evolved, particularly in the area of technology. Besides bringing benefits, this can also give rise to new or different risks.
- Supervisory bodies remain cognisant of these risks, and outsourcing continues to remain a priority topic.
- The ESMA Guidelines, specifically relating to Cloud Outsourcing*, is the latest effort from a European Supervisory Authority to provide detailed guidance on managing specific risks related to outsourcing.

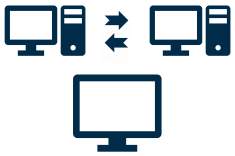
Non-exhaustive overview of recent regulatory initiatives covering outsourcing



*Final Report: Guidelines on outsourcing to cloud service providers (18 December 2020 | ESMA50-157-2403). The guidelines will be translated in the official EU languages and published by ESMA. The publication of the translations in all official languages of the EU will trigger a two-month period during which NCAs must notify ESMA whether they comply or intend to comply with the guidelines.

Supervisory concerns on outsourcing

1



Practical limitations

Recruiting, retaining and training employees with the relevant experience and skills to effectively manage the growing range of third-party ICT providers is a challenge for financial institutions (FIs) as well as for supervisory authorities overseeing them.

Challenges and issues relating to the ability of FIs to negotiate and exercise appropriate access, audit and information rights in outsourcing and third-party arrangements.

Limitations in the abilities of both FIs and supervisory authorities to identify the “nth-party risks” is a practical challenge.

2

Cross-border context

Access to a third-party in another jurisdiction by the relevant authorities, without creating unnecessary burden, conflict or duplication, is a challenge.

Supervisory and regulatory challenges can arise due to differing (or the lack of) data confidentiality standards and regulations that could hamper the sharing of information.

Limitations in relation to cooperation agreements and maturity of supervisions standards and priorities.

3

Concentration risk

A sufficiently large number of FIs (or a single systemic FI) can become dependent on one or a small number of outsourced or third-party service providers for the provision of critical services.

A major disruption, outage or failure at one of these third parties could create a single point of failure with potential adverse consequences for financial stability and/or the safety and soundness of multiple FIs.

Impact would depend on the specific services being provided, the criticality and substitutability of those services, and the mitigation plans in place.

Towards a more prescriptive regime on outsourcing

For further information, see further FSB ‘Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships (Discussion Paper, November 2020)

ESMA guidelines: Outsourcing to Cloud Services Providers

Developed to further Commission's FinTech Action Plan; aligned with EBA and EIOPA efforts.

Background

Help firms and competent authorities identify, address and monitor the risks and challenges arising from cloud outsourcing arrangements

Scope

- Will apply directly to, among other, Investments firms, AIFMs and UCITS management companies
- Regulatory basis significantly wide, including in AIFMD and MiFID
- While specifically introduced in relation to cloud will (likely) set standard for other forms of outsourcing

Application

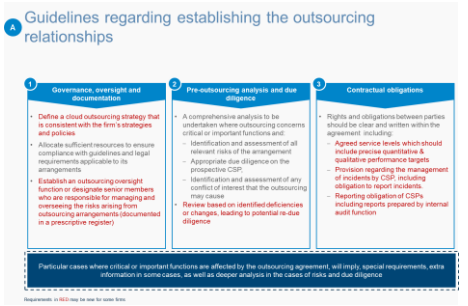
- 31 July 2021 for new, renewed or amended contracts
- 31 Dec 2022 for existing arrangements

Goal

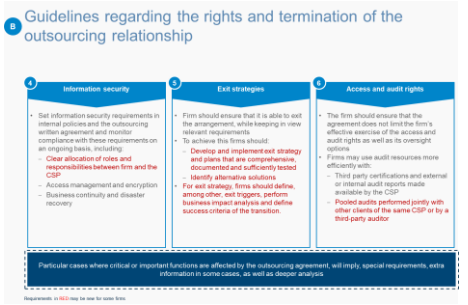
A harmonised approach towards outsourcing in financial services under different EU regimes

9 different guidelines impacting different aspects of the outsourcing process

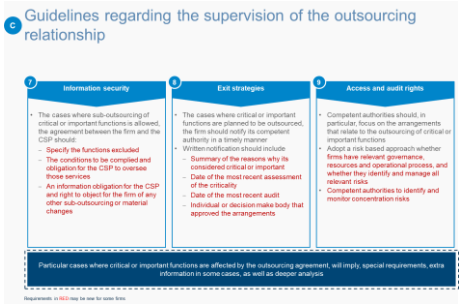
A **Establishing the outsourcing relationship**



B **Rights and termination of the outsourcing relationship**



C **Supervision of the outsourcing relationship**



A Guidelines regarding establishing the outsourcing relationships

Requirements in red may be new for some firms.

1 Governance, oversight and documentation

- Define a cloud outsourcing strategy that is consistent with the firm's strategies and policies
- Establish an outsourcing oversight function or designate senior members who are responsible for managing and overseeing the risks arising from outsourcing arrangements
- Assess and periodically reassess whether arrangements concerns critical or important functions
- Document all outsourcing arrangements in a register, with specific details for critical or important functions

2 Pre-outsourcing analysis and due diligence

- A comprehensive analysis to be undertaken where outsourcing concerns critical or important functions and:
  - Identification and assessment of all relevant risks of the arrangement
  - Appropriate due diligence on the prospective Cloud Service Providers,
  - Identification and assessment of any conflict of interest that the outsourcing may cause
- Review based on identified deficiencies or changes, leading to potential re-due diligence of the Cloud Service Provider

3 Contractual obligations

- Rights and obligations between parties should be clear and written within the agreement including:
  - Agreed service levels which should include precise quantitative & qualitative performance targets
  - Provision regarding the management of incidents by Cloud Service Providers, including obligation to report incidents
  - Reporting obligation of Cloud Service Providers including reports prepared by internal audit function

Outsourcing of critical or important functions will require, among other, stronger due diligence, detailed contractual terms, risk-based monitoring, and more prescriptive records to be maintained

B

Guidelines regarding the rights and termination of the outsourcing relationship

Requirements in red may be new for some firms.

4 Information security

- Set information security requirements in internal policies and the outsourcing written agreement and monitor compliance with these requirements on an ongoing basis, including:
  - Clear allocation of roles and responsibilities between firm and the Cloud Service Providers
  - Access management and encryption
  - Business continuity and disaster recovery

5 Exit strategies

- Firm should ensure that it is able to exit critical or important arrangements, while keeping in view relevant requirements
- To achieve this firms should:
  - Develop and implement exit strategy and plans that are comprehensive, documented and sufficiently tested
  - Identify alternative solutions
- For exit strategy, firms should define, among other, exit triggers, perform business impact analysis and define success criteria of the transition

6 Access and audit rights

- The firm should ensure that the agreement does not limit the firm's effective exercise of the access and audit rights as well as its oversight options
- Firms may use audit resources more efficiently with:
  - Third party certifications and external or internal audit reports made available by the Cloud Service Providers
  - Pooled audits performed jointly with other clients of the same Cloud Service Provider or by a third-party auditor

Outsourcing of critical or important functions will require, among other, a risk based approach towards information security, detailed exit strategies and planning, and well-calculated use of access and audit rights

C Guidelines regarding the supervision of the outsourcing relationship

Requirements in red may be new for some firms.

7 Sub-outsourcing

- The cases where sub-outsourcing of critical or important functions is allowed, the agreement between the firm and the Cloud Service Providers should:
  - Specify the functions excluded
  - The conditions to be complied and obligation for the Cloud Service Providers to oversee those services
  - An information obligation for the Cloud Service Providers and right to object for the firm of any other sub-outsourcing or material changes

8 Written notification to competent authorities

- The cases where critical or important functions are planned to be outsourced, the firm should notify its competent authority in a timely manner
- Written notification should include
  - Summary of the reasons why its considered critical or important
  - Date of the most recent assessment of the criticality
  - Date of the most recent audit
  - Individual or decision make body that approved the arrangements

9 Supervision of cloud outsourcing arrangements

- Competent authorities should, in particular, focus on the arrangements that relate to the outsourcing of critical or important functions
- Adopt a risk based approach whether firms have relevant governance, resources and operational process, and whether they identify and manage all relevant risks
- Competent authorities to identify and monitor concentration risks

Outsourcing of critical or important functions will require, among other, specific obligations on Cloud Service Providers in relation to sub-outsourcing, and notification to competent authorities along with a rationale behind the assessment

How is A&M assisting clients?

Given the anticipated timeline and high operational pressure, A&M is assisting clients in mobilisation though current state assessment and implementation strategies.

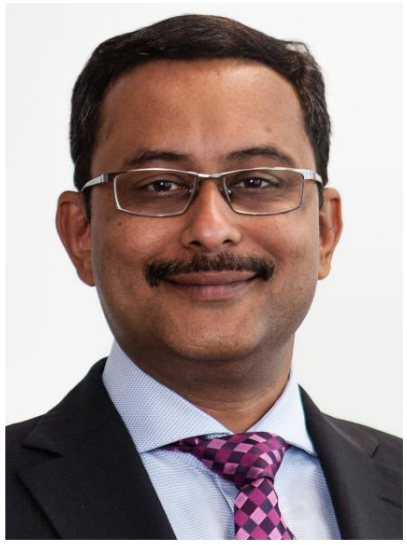
Assessing current arrangements in relation to

1. Strategy, governance and oversight
   - Evaluating outsourcing strategy, roles and responsibilities and controls
   - Assessing current maturity of outsourcing register (including identification of critical or important functions) and record keeping
2. Due Diligence and risk assessment
   - Assessing processes for onboarding and reviews
3. Accountability for the service provision and risk monitoring
   - Investigating level of reliance on outsourcing service provider
4. Information security and disaster recovery risks
5. Contractual limitations and lock-in risk
6. Business continuity and other operational risks
7. Legal risks including governing law of contract and data location
8. Supervisory access

Implementing change strategy through

1. Planning
   - Strategic choices in relation to implementation options (e.g. adopting group wide or localised policies, keeping in view extent of changes)
   - Based on scoping, defining Action Plan for high priority relationships which are directly impacted by regulatory changes
   - Presenting options for strategic implementation and action plan for lower priority outsourcing relationships and/or indirectly impacted relationships
2. Execution
   - Assisting in updating policies, procedures and registers in line with regulatory expectations while keeping in view the nature, scale and complexity of the business
   - Supporting in contract (re)drafting and (re)negotiations
3. Review
   - Setting up monitoring and review mechanisms through periodic testing and controls

A&M contacts



Angshuman Rajkhowa

Managing Director with Alvarez & Marsal's Financial Industry Advisory Services (FIAS) Practice in Amsterdam

+31 654 912 215

arajkhowa@alvarezandmarsal.com

Dr Zeeshan Mansoor

Director with Alvarez & Marsal's Financial Industry Advisory Services (FIAS) Practice in Amsterdam

+31 615 326 723

zeeshan.mansoor@alvarezandmarsal.com

"The information contained in this document is of a general nature and has been obtained from publicly available information plus market insights. The information is not intended to address the specific circumstances of an individual or institution. There is no guarantee that the information is accurate at the date received by the recipient or that it will be accurate in the future. All parties should seek appropriate professional advice to analyze their particular situation before acting on any of the information contained herein."

About Alvarez & Marsal

Companies, investors and government entities around the world turn to Alvarez & Marsal (A&M) for leadership, action and results. Privately held since its founding in 1983, A&M is a leading global professional services firm that provides advisory, business performance improvement and turnaround management services. When conventional approaches are not enough to create transformation and drive change, clients seek our deep expertise and ability to deliver practical solutions to their unique problems. With over 5,000 people across four continents, we deliver tangible results for corporates, boards, private equity firms, law firms and government agencies facing complex challenges. Our senior leaders, and their teams, leverage A&M's restructuring heritage to help companies act decisively, catapult growth and accelerate results. We are experienced operators, world-class consultants, former regulators and industry authorities with a shared commitment to telling clients what's really needed for turning change into a strategic business asset, managing risk and unlocking value at every stage of growth.

To learn more, visit: AlvarezandMarsal.com. Follow A&M on LinkedIn, Twitter, and Facebook.