afme/
Finance for Europe

CAPCO

Global Operating Approaches in Capital Markets

The benefits for enabling resilient and effective operations and technology services

September 2021

Association for Financial Markets in Europe
www.afme.eu

Disclaimer

AFME's *Global Operating Approaches in Capital Markets: The benefits for enabling resilient and effective operations and technology services* (the "Report") is intended for general information only and is not intended to be and should not be relied upon as being legal, financial, investment, tax, regulatory business or other professional advice. AFME doesn't represent or warrant that the Report is accurate, suitable or complete and none of AFME, or its respective employees shall have any liability arising from, or relating to, the use of this Report or its contents.

Your receipt of this document is subject to paragraphs 3, 4, 5, 9, 10, 11 and 13 of the Terms of Use which are applicable to AFME's website (available at http://www.afme.eu/en/about-us/terms-conditions) and, for the purposes of such Terms of Use, this document shall be considered a "Material" (regardless of whether you have received or accessed it via AFME's website or otherwise).

September 2021

Contents

Executive Summary

The paper explores the benefits of global approaches for providing operations and technology services in capital markets and the implications of trending EU and global policy, which risks driving localisation. The paper has been developed with members of the AFME Technology and Operations Committee[1] and subject matters experts from Capco.

- Banks use global approaches to provide operations and technology services across the various locations and markets in which they operate, bringing efficiency, resilience, regulatory, service and cost benefits
- However, policymakers have an increasing focus on the impact of financial markets becoming more globally interconnected. This focus could result in requirements on banks to localise operations and technology services and introduce barriers to global approaches. For example:
  - Reducing client service efficiency and product opportunities due to the increased costs and complexity of facilitating cross-border operations
  - Inhibiting digital transformation by limiting the value from cross-border technologies and data flows and discouraging innovation and investment
- Ultimately, this localisation would affect other policy objectives by increasing funding costs for clients and investors and reducing investment in more resilient technologies and operations
- Banks recognise that global governance must complement robust local entity compliance, governance, controls, and oversight. Appropriate arrangements are put in place within the regulatory framework and how banks provide global operations and technology services
- Collaboration between banks and policymakers will be essential to consider any future policy impacts on global operating approaches. A risk and principles-based approach is needed to consider the implications of more interconnected financial markets against the efficiency and benefits of how banks operate

"Policymakers have an increasing focus on the impact of financial markets becoming more globally interconnected"

1 https://www.afme.eu/divisions-and-committees/technology-operations

Global Operating Approaches in Capital Markets

The benefits for enabling resilient and effective operations and technology services

Introduction

This paper highlights the benefits of global operating approaches which banks use to deliver operations and technology services, irrespective of whether they are headquartered in the EU or elsewhere. A global approach allows banks to deliver efficiency, resilience, regulatory, service and cost benefits to their clients and the financial markets across the diverse geographic locations in which they operate.

However, there is a risk that emerging EU and global policy could require banks to replicate operations and technology services within specific locations or restrict their use of intragroup arrangements and third-party outsourcing. Other recent events, such as the COVID-19 pandemic, have also heightened the attention of policymakers on operating approaches and the resilience of capital markets.

Any future drive towards the localisation of operations and technology services would significantly challenge banks to serve the clients and markets in which they operate. This outcome would also run contrary to broader policy objectives (such as the EU Capital Markets Union[2]) which aims to establish more robust, liquid, and sustainable markets that benefit clients and investors regardless of their location.

It will be essential that any future policy, in the EU and globally, does not inadvertently impact the development of resilient, secure, and efficient operations and technology services in capital markets.

Structure and scope of the paper

Through interviews with members of the AFME Technology and Operations Committee (TOC)[3] and supported by subject matter expertise from Capco, this paper discusses banks' use of global approaches for providing operations and technology services[4], covering:

- An overview of banks global operating approaches;
- Use-cases and benefits for operations and technology services; and
- The impact of emerging policy and localisation.

The paper concludes with a call to policymakers to recognise the benefits of global operating approaches to ensure that any future legislation does not inadvertently impact a banks clients or the development of resilient, innovative, and efficient operations and technology in capital markets.

"Global operating approaches ensure the development of resilient, innovative, and efficient operations and technology in capital markets"

2 https://ec.europa.eu/info/business-economy-euro/growth-and-investment/capital-markets-union/what-capital-markets-union_en

3 https://www.afme.eu/Divisions-and-committees/Technology-Operations

4 This paper does not cover other global operating aspects, such as prudential requirements, legal entity structures, tax, financial risk management, or non-bank market participants such as financial market infrastructure (FMIs).

An overview of banks global operating approaches

This section provides a high-level overview of how a bank can structure its operations and technology services globally. While not exhaustive, it is important for understanding the benefits of global operating approaches in the next section.

Banks are highly complex organisations due to having a diverse geographic presence. A wide range of factors are considered by a bank in determining its global operating approach; fundamentally, the cohesion of the bank as a group is essential to serve clients globally and meet regulatory, compliance, security, and resilience expectations in the locations within which it may operate.

Bank structure and divisions

A bank is structured as an overall group and comprises various entities in multiple geographic locations (e.g. subsidiaries, branches, and affiliates). The group is the overall legal entity for the bank and is headquartered in its home jurisdiction. The main differences between a bank's entities are the extent to which the group wholly owns them and whether they are a separate legal entity. For example, subsidiaries are typically separate legal entities, whereas branches are not. Bank group structures exist on a broad spectrum in their level of centralised (e.g. branches) or decentralised (e.g. legally incorporated subsidiaries) approach[5].

Internally, a bank comprises multiple corporate divisions that are specific functions needed to serve the clients, markets, and locations in which the bank operates. Most divisions are managed centrally at a group and global level to provide the strategy, governance, compliance, risk management, and operational resilience required for the bank. Whilst not exhaustive, common divisions within a bank include:

- **Executive Office:** Defining the strategy and governance across all divisions, entities and activities
- **Global Markets:** Providing financial products to clients such as fixed income or equity
- **Investment Banking:** Advising and financing corporate clients such as for mergers and acquisitions
- **Treasury:** Managing the capital and liquidity requirements of the group
- **Compliance and Risk:** Managing risks and regulatory obligations
- **Operations:** Enabling the bank and its clients to manage, settle and transfer products and services
- **Information Technology (IT):** Developing and managing the banks applications and IT infrastructure

Each division can have many sub-divisions. For example, the Global Markets Division can be subdivided by the products and asset classes provided to clients (such as fixed income or equities). Other divisions, such as the Operations or IT Divisions, can be divided into specific services they provide. For example, a function within the IT Division could provide applications and IT infrastructure solely to an asset class within the Global Markets Division.

5 A bank legal entity is the establishment of a subset of the bank in a particular location that satisfies specific legal, regulatory, prudential, compliance and operational requirements in that location. For example, a bank legal entity may have specific conditions to ensure its recoverability in the event of a disruption to the entire group (e.g. capital requirements). The requirement for a bank to establish legal entities is determined by a wide range of factors and requirements (e.g. the bank strategy, client and market needs, physical presence, regulatory requirements, liability, and capital requirements).

Intragroup services and outsourcing

The divisions within a bank, such as the IT or Operations Divisions, also provide services to all divisions, known as intragroup arrangements. For example, the IT Division of an EU headquartered bank could provide cybersecurity services to some, or all, divisions of the bank across the geographic locations it supports. Most regulators regard intragroup arrangements as outsourcing. They are subject to the same regulatory framework applicable to the bank outsourcing services to a third-party service provider (e.g. governance and oversight, contractual management and service levels, risk management, exit planning)[6].

An intragroup arrangement can be wholly owned and managed within the bank. For example, the bank owns, runs, and maintains a proprietary trading platform centrally for all divisions and locations. Equally, the intragroup arrangement can be provided through a third-party provider. For example, the bank contracts a third-party service provider to manage its data centres, which is provided as an intragroup service for all divisions and locations. Figure 1 below shows how the location of an intragroup arrangement or third-party provider service can differ within the bank's global footprint.

Figure 1: **Intragroup and third-party service locations**

An intragroup or third-party outsourcing service can have three locational footprints based on where the service is provided:

- Onshore: Based in the location and time zone of the bank group (e.g. an EU-headquartered group using a third-party service provider based in the EU or providing an intragroup service to an entity in the EU)
- Offshore: Based outside of the location and in a much different time zone of the bank group or operating in a different legal and regulatory environment (e.g. an EU headquartered group using a third-party service provider in Singapore or providing an intragroup service to an entity in Singapore)
- Nearshore: Based close and in a similar time zone of the bank group (e.g. a Spanish headquartered bank using a third-party service provider in Poland or providing an intragroup service to a Polish entity)

Intragroup arrangements and third-party outsourcing can also include elements of sub-outsourcing. For example, a bank may outsource the management of an IT service (i.e. an email platform) to a third-party service provider that outsources other components to other service providers (i.e. the IT network required to provide the email platform). The bank remains responsible for all sub-outsourcing via the outsourcing agreement with the primary third-party provider (e.g. stipulating what parts of the service may be sub-outsourced depending on regulatory and internal requirements).

Service companies

Divisions within a bank, such as the Operations or IT Divisions, can also be provided as intragroup arrangements in the form of a service company (a ServCo[7]). A ServCo can provide a broad range of services (i.e. IT, operations, HR, facilities, legal and compliance) to one or more divisions and locations across the group or the group in its entirety. A ServCo can be a legal or non-legal entity within the group depending on its specific objective or needs (e.g. a legal entity ServCo can have specific continuity requirements, such as for recovery and resolution planning, in the event of a disruption to other parts of the group).

6 See Annex II for an illustration of a bank intragroup service arrangement

7 https://www.europarl.europa.eu/RegData/etudes/IDAN/2016/587376/IPOL_IDA(2016)587376_EN.pdf

The evolution of global operating approaches

As briefly shown, it is important to note the wide range of operating approaches and locations that a bank can use to provide operations and technology services across the group. Each bank has evolved its own operating approach based on the clients and markets they serve to achieve service, efficiency, resiliency and cost benefits and to meet regulatory and compliance requirements in each location in which it operates. Typically, a more centralised approach is preferred for banks within wholesale capital markets because of the flexibility it can provide to serve clients cross-border.

Discussions with AFME TOC members identified eight factors that have determined how bank's global approaches for operations and technology services have evolved (see Table 1 below). In summary, whilst AFME TOC members recognised cost as an important driver of change over the last 15 years (e.g. moving operations to lower-cost offshore locations), more recently, banks have adapted their operating approaches to achieve benefits for resilience, innovation, and client service.

However, AFME TOC members also highlighted that regulation in the EU and globally continues to be a significant determining factor in how global operating approaches continue to evolve. For example, ongoing assessment and requirements for EU banks to meet governance and management body obligations as part of the ECB Supervisory Review and Evaluation Process (SREP).

Table 1: **Factors determining banks' global approaches for operations and technology services**

Factor	Summary	Examples
Regulation	Ensuring regulatory expectations are met at group and entity level in each operating location	Group oversight of compliance to all regional and entity-specific requirements (e.g. MiFID, Dodd-Frank)
Governance	Improved transparency, collaboration and decision-making across the group and all entities	Defined management roles and responsibilities across group and entity operations functions to respond to regulatory and risk change
Resilience	Providing business continuity, disaster recovery and resilience in the event of disruption	Critical operations and technology services mapped to an entity level
Agility	Providing operational flexibility to adapt quickly in response to external changes	Quickly deploying remote-working technology across all entities to maintain operations during the COVID-19 pandemic
Efficiency	Increasing standardisation and efficiency of cross-border processes and IT systems	Group-wide platform and data standards for trade capture and reporting in each entity
Innovation	Building new capabilities that can be scaled across the group and entities	Using group centres of excellence (e.g. cloud computing or AI) to provide skills and best practice to individual entities
Cost	Ensuring operations and technology cost efficiency and returns on investment; protecting and growing new revenue opportunities	Allocating an overall group operating budget to entities based on market changes or demand
Client Service	Providing responsive and high quality client service and support	Locating an operations presence across entities that meets client service expectations in multiple time zones (e.g. a 'follow the sun' model)

Benefits for operations and technology services

This section provides examples of how banks provide operations and technology services through global approaches and their various benefits. This section concludes by discussing how banks continue to identify new opportunities to transform their global operating approaches for the future.

Global operating approach use-cases

From discussions with AFME TOC members, Table 2 below provides use-cases of how banks use a range of global operating approaches and the benefits these can bring for operations and technology services[8].

In summary, the use-cases show that global approaches allow banks to provide high-quality and resilient client service, take advantage of new technologies at scale, mitigate the risk of legacy systems, and prioritise investment in new capabilities and skills. Ultimately, these approaches form the basis of a bank's ability to provide access to a wide range of products and services to clients cross-border, increase operational efficiency, optimise capital and liquidity, manage risk, and meet group and entity supervisory, legal, and regulatory requirements.

Table 2: **Benefits of global operating approaches for operations and technology**

Focus area	Use-case	Summary	Benefits
Operations	**Client Operations**	Operations teams (e.g. supporting Client Collateral Management) based in a diverse set of geographic locations across the group that are managed at a global level	• 24/7 client coverage and flexibility for resiliency (e.g. disaster recovery events in a specific location) • Central oversight, reporting and controls to provide consistent client service • Increased speed and servicing opportunities by allowing local entity and client collateral management functions to interact within a location • Consolidated IT platforms and standards to manage operations to a consistently high-quality service level
Operations	**Controls Testing**	The testing and monitoring of operations functions controls (e.g. reconciliations) that is performed across multiple global teams through a central function	• Group and entity compliance risks mitigated in a single process that increase the efficiency and quality of testing across the bank • Lessons learnt in one entity are applied to other entities and the group to improve overall compliance • Global and centralised group control framework can compare entities across common KPIs
Operations	**Anti-Money Laundering**	Managing a central platform at the group level for transaction monitoring and investigations across all entities	• Global patterns of behaviour identified across all entities that can be addressed at a group level • Technology and expertise developed centrally to benefit all entities (e.g. adopting machine learning and artificial intelligence capabilities)
Operations	**Regulatory Reporting**	Group platforms and functions to manage a single source of data for meeting local entity and group reporting requirements (e.g. stress testing, liquidity management)	• Improved access and quality of data, and reduced time to develop reports and address any findings • Greater range of stress testing scenarios performed centrally that can identify and address any entity-level changes needed • Improved management decision-making through a consolidated view across the group
Technology	**Cybersecurity**	Operating cybersecurity capabilities on a global basis through a subset of local entity-based centres across the group	• 24/7 coverage of cybersecurity monitoring across the group and all entities • Increased effectiveness of the group to respond to cyber-threat actors operating cross-border • Central group expertise that reduces the risk of attack where sufficient skills cannot be sought within an entity location

8 Each use-case cab be applied to the various approaches outlined in section 1

Focus area	Use-case	Summary	Benefits
Technology	**Investment and Innovation**	Technology investment and innovation coordinated at a group level across each division and local entity	• Investment allocated to priority group and entity initiatives that bring the greatest client service and efficiency benefits • New technologies and capabilities quickly scaled across the group and entities (e.g. a group AI centre of excellence to provide capabilities for all local entities) • Increase efficiency, tracking and return on investment of global and entity-based digital transformation strategies
Technology	**Cloud Computing Adoption**	Developing a group cloud utility model and centre of excellence for providing compute service to all entities	• Reduced technology risk by migrating from end-of-life IT infrastructure and applications • Increased capacity to meet changes in demand (e.g. trade processing during periods of volatility) • Improved DR and resilience through use of multi-region failover of infrastructure • High security standards adopted across all entities that conform to a group framework • Reliance on the negotiating power of the group to ensure that the cloud service can meet regulatory requirements
Technology and Operations	**Operational Resilience and Risk Management**	Local entity monitoring of operational and technology risk and resilience, collated and managed via global frameworks and reporting dashboards	• Improved tracking and view of risk and operational resilience across the group, using standard KPIs, recovery times and scenario planning • Increased effectiveness of operations through global information sharing and lessons learnt • Local entity assessment of operational risk is consistent with a group framework and standard • Group approach to technology risk to enable consistent standards, process and controls to all technology services

Transformation of global operating approaches

Discussions with AFME TOC members highlighted how banks continue to transform their operating approaches to meet changing client and regulatory expectations, adopt new technologies and data-driven innovation, and increase the agility needed to respond to future opportunities or disruption.

For example, banks are undergoing IT simplification programmes to reduce duplicative systems, which will increase the standardisation and control over processes such as trade reconciliation or developing regulatory reports. Another example is banks adoption of cloud computing services. A bank can use third-party providers to implement a standard compute offering for the group and all entities, consolidating technical standards and reducing the time required to provision new IT services. Transformation activities, such as the examples identified, are essential for ensuring that banks remain efficient, resilient, and competitive in meeting client expectations and changing markets.

Recent events, such as the COVID-19 pandemic, have also identified new challenges and opportunities for banks global operating approaches. For example, during prolonged employee work from home, the resilience demonstrated by banks means that secondary disaster recovery (DR) sites in some primary locations may no longer be required or as effective in future disruptive scenarios. Discussions with AFME TOC members stated that they are likely to reduce their DR site footprints in future operating model location strategies. A second example is a potential for banks to embrace greater flexibility and remote working. The ability of banks to maintain productivity during the period of prolonged remote working has created opportunities to identify and attract new talent in locations that may be outside of existing locations.

The risks of emerging policy towards localisation

This section outlines a growing focus from policymakers on financial stability and resilience as financial markets become more interconnected[9], and the impact if banks are required to replicate operations and technology services across their global footprint. It will be important that policymakers take a proportionate and risk-based approach to global operating approaches, accounting for banks existing governance and controls, and broader policy objectives such as encouraging digital transformation.

A growing focus of policymakers on non-financial risks

Whereas the focus of policymakers has historically considered financial risks (e.g. credit risk), more attention is now being placed on non-financial risks (e.g. cybersecurity, third-party outsourcing). This is shown by a rapid increase in national, EU and global policy on outsourcing, operational resilience, data protection, and the use of third-party providers over the last three years[10]. Other events, such as the COVID-19 pandemic, have further heightened the attention of policymakers on the operating approaches and resilience of capital markets[11].

For example, the Financial Stability Board (FSB) November 2020 discussion paper[12] on outsourcing stressed a systemic risk if outsourcing services to some third-party service providers becomes concentrated (e.g. cloud service providers). In their May 2020 paper, IOSCO[13] stated that banks must effectively manage risks from the dependency on a service provider which provides outsourcing services to multiple other banks.

"It will be important that policymakers take a proportionate and risk-based approach to global operating approaches"

Within the EU, the 2020 digital finance package[14] has placed technology and data sovereignty[15] as a core pillar of the future European financial system. The intent is to reduce European reliance on non-EU technology and third-party providers and promote greater oversight over financial markets data and critical services. For example, the legislative proposal for a Digital Operational Resilience Act (DORA) proposes a wide range of measures on a bank's use of third-party providers and intragroup service arrangements (See Figure 2 below).

This growing focus and emerging policy on outsourcing and third parties are closely tied to data localisation where limitations are placed on a banks ability to locate and use data cross-border[16]. For example, within DORA, the limitation on the use of third-country providers could have an inadvertent impact by driving data localisation in the EU (e.g. requiring the storage and processing of data within the region).

The COVID-19 pandemic has also heightened the attention of policymakers on banks use of intragroup services, third-party services, and dispersed geographic locations. For example, the suitability and capacity of offshore operations when faced with restrictions on staff mobility. However, discussions with members of the AFME TOC stressed that the industry demonstrated significant resilience and agility to prevent any significant disruptions during this time.

9 https://blogs.worldbank.org/allaboutfinance/globalization-and-banking

10 See Annex 1 for a list of recent policy initiatives

11 https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/659617/IPOL_BRI(2020)659617_EN.pdf

12 https://www.fsb.org/2020/11/regulatory-and-supervisory-issues-relating-to-outsourcing-and-third-party-relationships-discussion-paper/

13 The International Organization of Securities Commissions (IOSCO)

14 https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

15 Technology and data sovereignty is a broad and strategic EU policy ambition within the 2020 digital finance package to ensure control over European computing power, data, and security to retain and promote European values and competition globally

16 https://www.irsg.co.uk/assets/Reports/IRSG_DATA-REPORT_Localisation.pdf

The ongoing implications of Brexit are also a focus of policymakers and regulators, which could impact further localisation of banks operations and technology within the EU. EU entities of a bank must already have governance and risk management commensurate with the nature, scale, and complexity of activities performed and compliance with existing EU legislation[17]. However, there is a risk that what is required for a physical presence increases over time due to a range of outcomes from the Brexit process (e.g. increasing the operational presence and the underlying technology and data within a location). This could, for example, include any new supervisory or legislative requirements or relocation of financial market infrastructures. Both the EU and UK regulators are also continuing to assess requirements for branches of international firms[18].

The risk of operations and technology localisation

Increased regulatory requirements towards localisation would require banks to replicate or duplicate operations and technology services in specific locations. This localisation would limit the economies of scale and benefits of global approaches and impact EU and global markets client service and resilience. Examples of the risks of localisation are outlined in Table 3 below using four use-cases from the previous section.

Table 3: **Risk of localisation for banks, clients, and EU and global markets**

Focus area	Use-case	Impact of localisation
Operations	**Client Operations**	• Reduced client service, quality, efficiency, and product opportunities (e.g. increased costs of funding or an inability to facilitate cross-border services) • Reduced resilience in the event of a service disruption (e.g. disaster recovery event) or market change (e.g. increased volatility)
Technology	**Cybersecurity**	• Increased competition for scarce skills in each entity location and the capacity to respond to a disruption (e.g. reduced single view of risks and event monitoring) • A wider attack surface for threat actors to exploit (e.g. duplicate IT infrastructure, roles, and functions across locations)
Technology	**Cloud Computing Adoption**	• Duplication of controls and on-premise and cloud infrastructure (e.g. reduced resiliency benefits of cross-border deployment models for managing data and workloads) • Reduced ability to store and transmit data cross border (e.g. producing consolidated group compliance or regulatory reports to identify and remediate issues)
Technology and Operations	**Operational Resilience and Risk Management**	• Reduced service quality and efficiency (e.g. increased costs of funding; an inability to facilitate cross-border services) • Reduced resilience in the event of a disruption due to the concentration risk of operations or technology service localisation (e.g. a disaster recovery event)

This trend towards localisation would counter other policy ambitions, such as the EU digital finance package and Capital Markets Union (CMU). For example, more significant localisation would inhibit banks from developing new technologies at scale in the EU market, such as artificial intelligence, by placing barriers on global operating arrangements (e.g. the ability to use a ServCo or Centre of Excellence for the efficient use of resources and scarce skills to develop the technology). A further example of the localisation risk for banks intragroup arrangements is shown in Figure 2 below.

17 https://www.bankingsupervision.europa.eu/banking/relocating/html/index.en.html

18 https://www.eba.europa.eu/eba-proposes-further-harmonise-eu-law-applicable-branches-third-country-credit-institutions

Figure 2: **The EU DORA localisation risks for operations and technology services**

EU Digital Operational Resilience Act

The 2020 EU DORA proposes legislative measures across IT risk management, incident testing and reporting, and the direct oversight of critical third-party providers. However, it is unclear to what extent:

- A bank's intragroup arrangements fall within the definition of an 'ICT third-party provider' or 'critical third-party provider' (i.e. understood to mean an entirely separate institution that provides services to a bank, such as a cloud service provider),
- EU financial entities can rely on intragroup arrangements within their bank group, located outside the EU, to demonstrate compliance with DORA,
- If a bank group outside of the EU can provide intragroup arrangements to external parties within the EU (e.g. entities outside the group, such as another bank), and
- The ability for an EU entity to use a third-parties that are not based, or have a legal presence, in the union.

Potential impacts on banks intragroup arrangements

Banks intragroup arrangements are subject to the same regulatory requirements as the overall bank group (e.g. senior management oversight, compliance and controls frameworks, prudential requirements). Further, intragroup arrangements are regulated by relevant EU national competent authorities (NCAs) in which their services are located and used (e.g. at a group and entity level). Therefore, any risks from global banks intragroup arrangements are already supervised within the EU, irrespective of whether services are provided exclusively with the bank group or to external parties. See Annex II for an illustration of a bank intragroup service arrangement.

There are various supervisory frameworks that apply to global banks to ensure EU regulators have oversight of operations and technology services at the local and group level. For example, a non-EU headquartered bank operating within the EU falls under the ECB Single Supervisory Mechanism (SSM) and the relevant NCAs in the location where its entity is based. The EU entity is also subject to EU ESA guidelines regarding IT management and outsourcing and delegation of any services via intragroup arrangements with the bank group outside of the EU.

Including intragroup arrangements within the DORA definition of an ICT provider, or critical ICT provider, would subject the bank to a new and duplicative supervisory framework (e.g falling under DORA and existing NCA requirements). This would require banks to establish localised technology functions to undertake activities within the EU. This localisation would fragment a bank's group-wide operations and technology functions resulting in cost and efficiency increases that would reduce the service, security, and resilience benefits that global operating approaches, such as intragroup, provide.

Finally, localisation would have implications for the efficiency of a bank's allocation of capital and liquidity, with the aggregate amount of capital and liquidity held through localised entities likely to exceed that required to cover the same risks if these were met by the group on a consolidated basis. This fragmentation resulting from separate pots of capital and liquidity leads to inefficiencies by increasing banks' cost of capital and funding, resulting in a lower supply or higher cost of financing for businesses and lower returns for savers and investors. With restrictions often preventing the free transfer of resources across groups, these measures would further risk increasing the financial fragility of banking systems particularly at times of stress while, at least in Europe, undermining progress towards a genuine Banking Union.

Recognising the benefits of global operating approaches

In developing this paper, members of the AFME TOC acknowledged the concerns of EU and global policymakers regarding the reliance of banks on global operating approaches. In that respect, global policies must be complemented by robust local entity compliance, governance, controls and oversight, to allow local entities to rely on other parts of the group, especially where there are sub-outsourcings. For example, banks operating in the EU must ensure that outsourcing arrangements are documented on robust contractual and compliance requirements relevant to existing regulations[19]. EU financial entities retain full responsibility for their compliance and oversight to relevant NCAs in the locations they are based.

The cohesion of banks at a global level is fundamental to serving clients cross-border and meeting regulatory expectations on common standards, controls, and risk management. It will be essential that future legislation does not inadvertently impact the development of resilient, secure, and efficient capital markets by seeking to replicate operations or technology services in each location in which a bank operates.

Members of the AFME TOC emphasised that collaboration between banks and policymakers will be essential to consider the impacts of future legislation on global operating approaches. This will account for the controls and regulatory frameworks banks are already subject to and the ability to continue relying on third-party outsourcing, or intragroup arrangements, at a group level.

Maintaining a risk and principles-based approach, proportionate to banks existing use of global operating approaches, will be essential in achieving policymakers' broader aims of developing more resilient, digital, and innovative capital markets.

"Global policies must be complemented by robust local entity compliance, governance, controls and oversight"

19 Complying with the recent EBA Guidelines on Outsourcing which cover extensively the governance arrangements required for third-party outsourcing and intragroup arrangements (such as due diligence and risk assessments, contracting, audit, business continuity and exit planning).

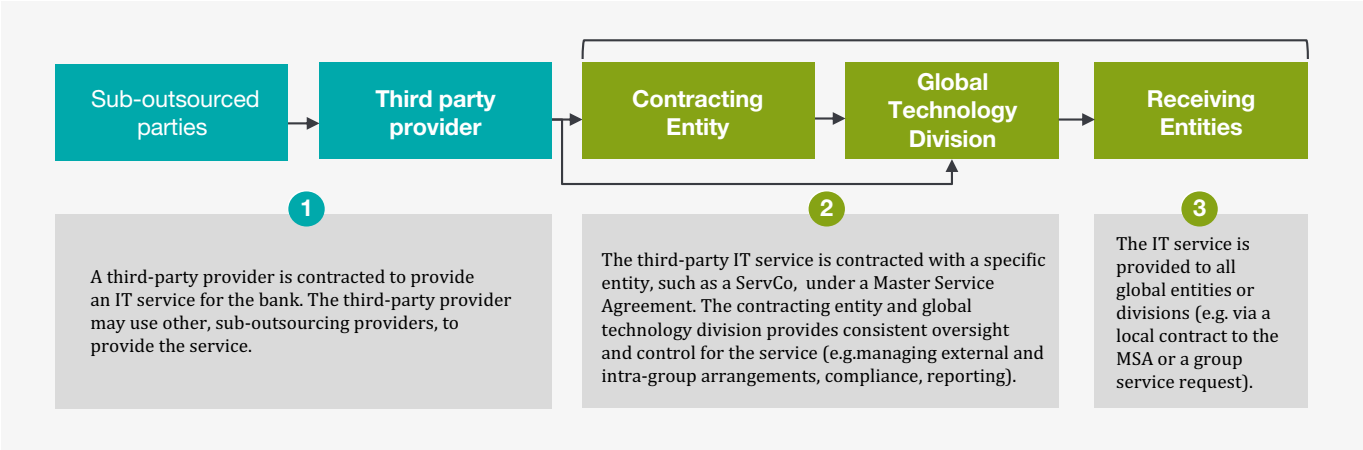
Annex I

Recent EU and global policy with implications for global operations and technology (noting that not all of the regulators listed have stated requirements towards localisation).

Published	Jurisdiction	Authority	Policy
2019	EU	EBA	Guidelines on outsourcing arrangements
	Global	FSB	Third-party dependencies in cloud services: Considerations on financial stability implications
2020	EU	European Commission	Proposal for a digital operational resilience act (DORA)
	EU	ESMA	Guidelines on outsourcing to cloud service providers
	Global	IOSCO	Principles on Outsourcing
2021	UK	FCA/BoE/PRA	Operational Resilience: Impact tolerances for important business services
	UK	PRA	Outsourcing and third-party risk management
	IE	CBI	Cross Industry Guidance on Operational Resilience and Outsourcing
	US	Federal Reserve	Sound Practices to Strengthen Operational Resilience
	US	FRB/FDIC/OCC	Proposed Interagency Third-Party Risk Management Guidance
	Global	OECD	Global value chains: Efficiency and risks in the context of COVID-19
	Global	FSB	Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships
	Global	BIS	Principles for operational resilience

Annex II

Figure 3: **A generic IT intragroup service that is provided globally across a bank group.**



The illustration shows how a bank can provide access to a range of services to clients cross-border, manage risk, and meet group and entity supervisory, legal, and regulatory requirements (see benefits in Table 2 of his paper). The risk of emerging policy towards localisation would fragment a bank's group-wide operations and technology functions and reduce the service, security, and resilience benefits that global operating approaches, such as intragroup, provide.

Contributors

We are grateful to our Technology and Operations Committee member firms and the individuals who contributed their time and input for producing this paper.

AFME Technology and Operations

AFME's Technology and Operations Division brings together senior technology and operations leaders to influence and respond to current pan-European market drivers and policy. Find out more at www.afme.eu/Divisions-and-committees/Technology-Operations.

Global Operating Approaches in Capital Markets: The benefits for enabling resilient and effective operations and technology services was led by the AFME Technology and Operations Committee as an initiative within the broader Technology and Operations Division.

About Capco

Capco is a global technology and management consultancy specializing in driving digital transformation in the financial services industry. With a growing client portfolio comprising of over 100 global organizations, Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its Innovation Labs, and award-winning Be Yourself At Work culture and diverse talent. To learn more, visit www.capco.com or follow us on Twitter, Facebook, YouTube, LinkedIn, Instagram, and Xing.

Contacts

AFME

Andrew Harvey
Managing Director
Technology and Operations
andrew.harvey@afme.eu
+44 (0)203 828 2694

David Ostojitsch
Director
Technology and Operations
david.ostojitsch@afme.eu
+44 (0)20 3828 2761

Capco

Tej Patel
Partner, FRC
tej.patel@capco.com
+44 (0) 7968 977 137

David Turmaine
Executive Director, Post Trade
david.turmain@capco.com
+44 (0) 7809 231 115

/ About AFME

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues.

We represent the leading global and European banks and other significant capital market players.

We advocate for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society.

We aim to act as a bridge between market participants and policy makers across Europe, drawing on our strong and long-standing relationships, our technical knowledge and fact-based work.

Focus
on a wide range of market, business and prudential issues

Expertise
deep policy and technical skills

Strong relationships
with European and global policymakers

Breadth
broad global and European membership

Pan-European
organisation and perspective

Global reach
via the Global Financial Markets Association (GFMA)

afme/
Finance for Europe

London Office
39th Floor
25 Canada Square
London, E14 5LQ
United Kingdom
+44 (0)20 3828 2700

Brussels Office
Rue de la Loi, 82
1040 Brussels
Belgium
+32 (0)2 788 3971

Frankfurt Office
Neue Mainzer Straße 75
Bürohaus an der Alten Oper
60311 Frankfurt am Main
Germany
+49 69 153 258 963

Press enquiries
Rebecca Hansford
Head of Media Relations
rebecca.hansford@afme.eu
+44 (0)20 3828 2693

Membership
Elena Travaglini
Head of Membership
elena.travaglini@afme.eu
+44 (0)20 3828 2733

Follow AFME on Twitter
@AFME_EU