association of the luxembourg fund industry

IOSCO Consultation

Principles on Outsourcing

ALFI response

30 September 2020

About ALFI

The **Association of the Luxembourg Fund Industry (ALFI)** represents the face and voice of the Luxembourg asset management and investment fund community. The Association is committed to the development of the Luxembourg fund industry by striving to create new business opportunities, and through the exchange of information and knowledge.

Created in 1988, the Association today represents over 1.500 Luxembourg-domiciled investment funds, asset management companies and a wide range of businesses that serve the sector. These include depositary banks, fund administrators, transfer agents, distributors, law firms, consultants, tax advisory firms, auditors and accountants as well as specialist IT and communication companies. Luxembourg is the largest fund domicile in Europe and a worldwide leader in cross-border distribution of funds. Luxembourg-domiciled investment funds are distributed in more than 70 countries around the world.

We thank IOSCO for the opportunity to participate in this consultation.

Introduction
Objective, approach, items for consideration

Context

IOSCO issued a consultation requesting feedback on proposed updates to its principles for regulated entities that outsource tasks to service providers.

https://www.iosco.org/library/pubdocs/pdf/IOSCOPD654.pdf

Since the publication of IOSCO´s earlier principles (*2005* and *2009 links*) on outsourcing for market intermediaries and for markets, developments in markets and technology have increased regulatory attention on risks related to outsourcing and the need to ensure the operational resilience of regulated entities.

The revised principles comprise a set of fundamental precepts and a set of seven principles. The fundamental precepts cover issues such as the definition of outsourcing, the assessment of materiality and criticality, their application to affiliates, the treatment of sub-contracting and outsourcing on a cross-border basis. The seven principles cover the following areas:

1. Due diligence in the selection and monitoring of a service provider
2. The contract with a service provider
3. Information security, business resilience, continuity and disaster recovery
4. Confidentiality issues
5. Concentration of outsourcing arrangements
6. Access to data, premises, personnel and associated rights of inspection
7. Termination of outsourcing arrangements

Approach

In the next pages, for each of the 13 questions contained in the consultation, this document combines:

- **A summary of assumptions proposed in the consultation, followed by the corresponding question**
- **The response prepared by ALFI**

Scope of the consultation
Dimensions to take into account

1. Transactions

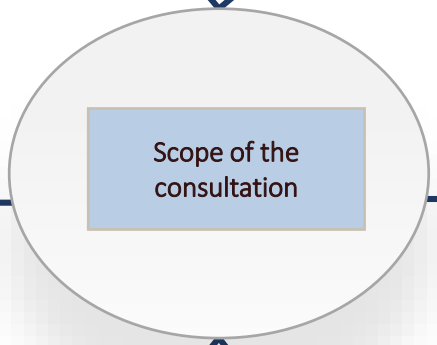
- Market transactions
- Underlying = securities and derivatives, UCI, in particular having ISIN

2. Functions

- Information technology (IT),
- Operation/support of exchanges and trading platforms,
- Regulatory reporting,
- Other control functions such as real-time trade monitoring and audit

3. Benefits

- Access to expertise at a lower cost
- Automation
- Cost efficiency



4. Risks / Concerns

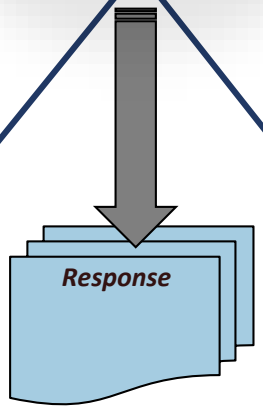
- Resilience in operational activities and business continuity maintenance
- Compliance (outsourcing to entities that are not regulated and/or based in different jurisdictions)
- Concentration in a small number of companies

5. Geography

- Outsourcing to a different jurisdiction
- Intercompany aspects
- Third-country aspects

6. Provider / Sourcer

- IT based companies
- Joint ventures
- Strategic alliances



Questions asked in the consultation
Summary

Section	Question
PRECEPTS	*Q1: Do you consider the **scope of the application** of the Principles to entities is clear? If not, why not?*
	*Q2: Do you consider the **concepts used to explain the application** of the Principles on Outsourcing to be clear and adequate? If not, why not?*
	*Q3: Do you have any comments on the **benefits, risks, and challenges** of the use of outsourcing? Are there any additional factors which should be considered or described in the document?*
	*Q4: Does the description of **materiality and criticality** clearly and adequately address the proportional application of these principles? If not, why not?*
Principle 1	*Q5: Do you consider the Principle and implementation measures for **due diligence** are adequate and appropriate? If not, why not?*
Principle 2	*Q6: Do you consider the Principle and implementation measures for **establishing the contract with a service provider** are adequate and appropriate? If not, why not?*
Principle 3	*Q7: Do you consider the Principle and implementation measures for **information security, business continuity and disaster recovery** are adequate and appropriate? If not, why not?*
	*Q8: What measures for **business continuity would be effective in situations where all, or a significant portion, of both the outsourcers' and third-party providers' work force is working remotely**? In particular what steps should be taken with respect to **Cyber Security and Operational Resilience**?"*
Principle 4	*Q9: Do you consider the Principle and implementation measures for the **management of confidentiality issues** are adequate and appropriate? If not, why not?*
Principle 5	*Q10: Do you consider the Principle and implementation measures for the **management of concentration risk in outsourcing arrangements** are adequate and appropriate? If not, why not?*
Principle 6	*Q11: Do you consider the Principle and implementation measures for **ensuring access arrangements** are adequate and appropriate? If not, why not?*
Principle 7	*Q12: Do you consider the Principle and implementation measures for **the termination of outsourcing arrangements** are adequate and appropriate? If not, why not?*
	*Q13: Do you have **any other comments** on the Principles and implementation measures? Do you have any suggestions for other areas or risks IOSCO should address?*

Chapter 2 - Background
Context

1. Outsourced Tasks

There is a wide range of tasks that are outsourced in the securities and derivatives markets. Commonly outsourced tasks include information technology (IT), operation/support of exchanges and trading platforms, regulatory reporting, and other control functions such as real-time trade monitoring and audits. Other examples include joint ventures and strategic alliances aimed at facilitating trading (e.g., the shared use of analytical, legal, compliance, internal controls, IT, and any other support functions for critical tasks within a group of entities).

In the over-the-counter (OTC) derivatives sector, outsourced post trade tasks typically include trade matching and confirmation, portfolio reconciliation and compression, collateral management, trade reporting, credit limit checks, and custody of assets.

2. What is at stake ?

It is increasingly commonplace for firms to use third party service providers to carry out, or otherwise support, some of their regulated business activities. While this approach can deliver economic benefits, it may also raise concerns about risk management and compliance when such tasks are outsourced to entities that are not regulated and/or are based in different jurisdictions. In particular, it can diminish regulators' ability to regulate or supervise certain functions within firms.

3. Observations from industry participants

Members of the Committees participating in this work surveyed or consulted industry participants in their respective jurisdictions and sectors for information regarding current outsourcing practices and how they have been impacted by recent changes. After their information gathering exercises, some IOSCO members reported that outsourced tasks are, in parts of some markets, concentrated in a small number of highly specialised, often IT-based companies. Consequently, some IOSCO members are concerned that disruption to the functioning of these companies could constitute a source of risk in the areas they serve. Therefore, although outsourcing may bring substantial benefits to markets and their participants, it poses a number of important and evolving challenges and may have an impact on the effectiveness and integrity of markets.

Chapter 3 – Fundamental precepts
A. Scope of application

The Principles on Outsourcing should apply to those regulated entities that are within the scope of the IOSCO Committees 2, 3, 6, and 7; namely, trading venues, market intermediaries and market participants acting on a proprietary basis, credit rating agencies, and financial market infrastructures that are regulated under the relevant legal regime of a jurisdiction. More specifically, for the purposes of this report:

i. Trading venues	"trading venues" generally refers to exchanges or other multilateral trading facilities including, for example, alternative trading systems (ATSs) and multilateral trading facilities (MTFs). It also refers to the operator of a particular trading venue. IOSCO recognises that the concept of a "trading venue" differs among IOSCO member jurisdictions and the concept may, at the discretion of individual members (for their jurisdictions only) also include other types of trading venues referred to by alternative nomenclatures.
ii. Market intermediaries and market participants	"market intermediaries and market participants" is applied as appropriate in the context of jurisdictional differences in regulatory scope and generally refers to those regulated entities, other than those that are trading venues, that are in the business of some or all of the following: • executing orders in, or distributing, securities or derivatives; • proprietary trading or dealing on own account; • receiving and transmitting orders from or to third parties; • providing advice regarding securities or derivatives or the advisability of purchasing or selling securities or derivatives; and • underwriting of new issues or products. Some jurisdictions may regulate an entity as a market intermediary that simply provides advice regarding the value of securities or derivatives or the advisability of investing in, purchasing or selling such instruments.
iii. Credit risk agency	"credit rating agency" or "CRA" means an entity that is in the business of issuing credit ratings. "Credit rating" or "rating" means an assessment regarding the creditworthiness of an entity or obligation, expressed using an established and defined ranking system.
iv. Financial market insfrastructures	"financial market infrastructures" means multilateral systems among participating institutions, including the operator of the financial market system, used for the purposes of clearing or settling or recording securities, derivatives, or other financial transactions, and trade repositories, entities which are defined as financial market infrastructures[4] and other regulated entities which may report or retain regulatory data.
Question 1	*Do you consider the scope of the application of the Principles to entities is clear? If not, why not?*

ALFI's Response to question 1

1. We rather agree with the proposed principles and measures.

2. Nevertheless we would like to share the following comments.

a. Regarding point ii), we recommend to mention that « Securities » include « UCIs » (mutual funds), for sake of clarification and proper understanding.

b. UCITS funds and alternative investment funds (AIFs) with their corresponding managers fall within the scope of the IOSCO guidelines. Unregulated entities should be considered are out of scope.

c. Activities: Portfolio management activities are performing the trading transactions.

d. The scope of the application of the Principles is clear, but it might be interpreted as a focused and narrow definition not taking into account other applicable sets of outsourced tasks (e.g. distribution of financial products). The principles for market intermediaries and market participants should be elaborated clearer (e.g. with exemplary descriptions of functions).

e. A third-party should be understood as an agent not involved in the outsourcing arrangement (e.g. fund distribution agent, depositary bank, tri-party-collateral agent).

f. Dealing on own account should be understood as on behalf of the fund, and not proprietary trading. The implementation of outsourcing is part of the delegation, and should not create an additional useless layer of contractual relationship.

Chapter 3 – Fundamental precepts
B. Outsourcing

In this Consultation Report "outsourcing" is considered to be a business practice in which a regulated entity uses a service provider to perform tasks, functions, processes, services or activities (collectively, "tasks") that would, or could in principle, otherwise be undertaken by the regulated entity itself. This may also be referred to as onshoring, offshoring, near-shoring or right-shoring, depending on the organisational context and the relationship with affiliates and service providers.

Service provider

The term "service provider" is used throughout the Principles on Outsourcing to refer to both third party and affiliate service providers, regulated (whether or not by the same regulator with authority over the regulated entity) or unregulated.
The service provider may itself either be regulated (whether or not by the same regulator with authority over the regulated entity), or unregulated.

Outsourcing

Outsourcing may include tasks that the regulated entity has not previously performed, where those tasks would reasonably be expected to be initiated by the regulated entity if they had not been outsourced to a third party. Outsourcing may also include tasks that the regulated entity does not have the capacity or resources to perform. This may occur in particular when a new regulated entity is established, or when an existing regulated entity enters a new area of business or becomes subject to a new regulatory requirement.
For the purpose of these Principles, further transfers of an outsourced task (or a part of that task) from one service provider to another are referred to as "subcontracting". In some jurisdictions, the initial outsourcing by the regulated entity may be referred to as subcontracting. For the purposes of this document, the difference between outsourcing and subcontracting is explained in Fundamental Precept I. Outsourcing does not cover purchasing contracts. Purchasing is defined as the acquisition from a vendor of services, goods or facilities without the transfer of, access to, or responsibility for the handling of the purchasing entity's non-public proprietary or client information. For example, a trading venue may choose to use a service provider for the publication of executed trades, and it may also use an external provider of training services for its staff. The former would be considered an outsourcing arrangement whereas the latter would be a purchasing contract.

Question 2

Do you consider the concepts used to explain the application of the Principles on Outsourcing to be clear and adequate? If not, why not?

ALFI's Response to question 2

We welcome the clarity that IOSCO aims at providing market participants with in relation to the definition of "outsourcing". We see a valuable benefit in clarifying and harmonising terminologies and practices across on-shoring and off-shoring models.

Nevertheless, we are of the view that the IOSCO definition of Outsourcing encloses the concept of Delegation which is largely used within the asset management industry and regulation. We would appreciate a clarification between these two concepts: Outsourcing and Delegation. Purchasing is applicable to the acquisition of point in time services such as training and consulting.

By way of illustration, it is worth mentioning that the European Banking Authority's Guidelines on outsourcing arrangements (EBA/GL/2019/02) provide examples of what should not be considered outsourcing (please refer to paragraph 28 of the GL). We would welcome from IOSCO common sense examples of what is considered delegation, what constitutes outsourcing and what corresponds to purchasing.

We share IOSCO's view that outsourcing does not cover purchasing contracts or the acquisition of services that would not, or could not in principle, otherwise be undertaken by the regulated entity itself.

A contract will be necessary irrespective of the service provided / acquired, therefore "subcontracting" is not exclusive to the question of outsourcing. Whilst "subcontracting" is going to be a feature for further transfers of outsourced task, we believe that one should refer to "sub-outsourcing" to simplify terminologies used. Sub-outsourcing is the transfer of task or service defined as outsourcing from an original outsourcing partner to another third party.

A regulated entity will supervise / monitor risks stemming from an outsourcing chain, which is already a notion in force with some regulatory authorities.

Chapter 3 – Fundamental precepts
C. Responsibility for outsourcing

Responsibility Liability Accountability	The regulated entity retains full responsibility, legal liability, and accountability to the regulator for all tasks that it may outsource to a service provider to the same extent it would if the service were provided in-house. The regulatory responsibilities of the regulated entity and its management cannot be outsourced. Moreover, outsourcing should not be permitted to impair the regulator's ability to perform its functions, including the proper supervision and examination of a regulated entity.
Management and the governing body	Management and the governing body of the regulated entity should develop and implement appropriate policies and procedures reasonably designed to achieve the objectives of these Principles, to periodically review the effectiveness of those policies and procedures, and to address any identified outsourcing risks in an effective and timely manner.
Implementation of the Principles on Outsourcing	Regulated entities should also be aware of and comply with mechanisms within their jurisdiction that may have been put in place to implement these Principles on Outsourcing. Such mechanisms may take the form of government regulation, regulations, guidelines, codes, or practices imposed by non-government statutory regulators, industry codes, guidelines or practices, or some combination of these items.
Regulators expectations	Regulators expect to have prompt complete physical or electronic, or remote access to data concerning a regulated entity's activities, whether such data are in the custody of the regulated entity's service provider or otherwise.

D. Potential benefits of Outsourcing

Examples of substantial benefits

Outsourcing by the financial services industry can provide a number of substantial benefits. For example, it:

• Permits financial entities to obtain necessary expertise at a lower cost than might be possible by hiring internal staff and allows entities to focus on their core business. By lowering costs, outsourcing may also permit smaller entities and start-up companies to break into established markets and increase competition which benefits end users.

• Helps automate and speed up tasks, reduce the need for manual intervention and assist in minimising operational risks. This has undoubtedly brought efficiencies to trading, settlement and post trade processing and is now critical to healthy and efficient markets. It may even make viable the business models of smaller entities.

• Provides flexibility to the business models of regulated entities, by enabling them to rapidly adjust both the scope and the scale of their activities to meet client, market, or proprietary imperatives. Outsourcing permits entities to concentrate on the regulated activities they

Use of cloud-based services or infrastructure

One example of the potential benefits of outsourcing is evident in the use of cloud-based services or infrastructure. Based upon C6's interactions with cloud computing experts, proponents of cloud-based infrastructures highlight several advantages:

• Improved accessibility – Services are accessible from a wide variety of devices and from any location with network access to the cloud.

• Cost efficiency – Cloud provider resources are pooled to serve multiple clients, which creates economies of scale. This reduces the cost of data storage.

• Demand scalability – The cloud provides a flexible platform that can grow and shrink to match the client's needs.

• Always-on availability – Applications running on a cloud infrastructure are rarely off-line and are accessible whenever there is an internet connection.

• Improved security – A key concern of a cloud provider is to carefully monitor the cloud's security, which is more efficient than monitoring a conventional in-house system.

Chapter 3 – Fundamental precepts
E. Potential risks and challenges

Outsourcing poses a number of challenges and risks, both for regulated entities that outsource and for their regulators.

Control	When a regulated entity uses a third party to perform a task, it may have a detrimental impact on the regulated entity's understanding of how the task is performed, with a consequential loss of control over that task. A regulated entity may lack control over some outsourced tasks, hindering its ability to protect the confidentiality of its own and client information. This risk has increased in recent years, as many tasks are being digitalised and/or based on algorithms, and data and information are stored in cloud environments, i.e., stored on remote servers and accessed from the internet. It is common industry practice to use privacy agreements when outsourcing tasks to safeguard data.
Data and Technology	It is generally accepted that the number of cyber incidents and data leaks is increasing. Further, the inappropriate selection of a service provider may lead to a business disruption, with negative consequences for the regulated entity's clients and, in certain instances, the potential for spill-over effects and systemic risk to the market as a whole. Outsourcing to, and storing of, data in a cloud may increase certain risks, such as the risk of cyber incidents. This could make the monitoring of, and reliance on, outsourced tasks more difficult due to: the uncertainty of the physical location of data, a possible lack of understanding of cloud technology risks on the part of the regulated entity, and the rapid development and changing nature of cloud technology. However, the adoption of cloud technology by regulated entities may have a mitigating impact on these risks: Cloud service providers may be more aware of cyber-security issues and have more sophisticated systems to detect and prevent cyber-incidents than local data centre providers or individual regulated entities.
Operational resilience	Operational disruptions to the services a regulated entity provides have the potential to harm consumers and market participants, to threaten the viability of regulated entities, and to cause instability in the financial system. The term operational resilience refers to the ability of regulated entities, other firms such as service providers, and the financial market as a whole to prevent, respond to, recover, and learn from operational disruptions. There are numerous challenges to ensuring the businesses of regulated entities are resilient to operational disruption. These challenges have become more complex and intense in recent years, a period of technological change and an increasingly hostile cyber environment. Additional challenges occur where firms operate internationally or outsource a significant level of tasks to third parties. Low resilience may represent a threat to regulators' objectives to protect investors, ensure market integrity, and maintain financial stability. Consequently, the operational resilience of regulated entities is a priority for regulatory authorities that is no less important than financial resilience. Given the increasing interconnectedness of international markets, the development of common principles on outsourcing help ensure that operational resilience is not adversely affected by the location of the regulated entity's service providers and will facilitate regulatory 10 co-operation in the supervision of regulated entities operating internationally. Furthermore, common operational resilience principles might also be good for competition because common minimum standards may help new entrants establish themselves in a market.

Chapter 3 – Fundamental precepts
E. Potential risks and challenges

Concentration	Service providers have become more specialised in recent years, leading to situations where only a few entities offer certain (often IT-dependent) services. As a result, concentration in the number and/or materiality of the services that are outsourced may have increased. This concentration may weaken competitive pressures on service providers, potentially reducing their incentives to improve service and resilience levels or to price competitively. In addition, the lack of competition may lead to under-investment in risk management, systems, and operational innovation, ultimately reducing the resilience and efficiency of the overall market. However, there were different views on the problems of concentration. Although they reported limited competition in some post-trade services, some regulated entities viewed concentration of service providers as beneficial to the market. They expressed concern that regulatory action, such as reducing barriers to entry, may force established firms in markets that have a tendency to concentrate (e.g., those with significant economies of scale or network effects) to leave those markets. This would then have negative consequences for users. However, other regulated entities reported that service providers with a "market-controlling" position often refuse to agree on contractual provisions that are necessary for the regulated entity to comply with jurisdictions' regulatory requirements or to agree with contractual inspection rights for regulated entities and their regulators. Possible operational and systemic risks also may arise if multiple regulated entities use a common service provider.
Supervisory	Outsourcing may pose important challenges to the integrity and effectiveness of financial services regulatory and supervisory regimes and systems. A regulated entity may lose some control over the people and processes dealing with the outsourced tasks. Nonetheless, regulators require that the regulated entity, including its board of directors and senior management, remain fully responsible (to clients and regulatory authorities) for the outsourced task as if the service were being performed in-house. In some jurisdictions, regulators may prohibit or impose restrictions or notification requirements on the outsourcing of certain tasks where the jurisdictions have determined that outsourcing introduces an unacceptable risk or is critical to the functioning of a regulated entity or the integrity of the market.
Question 3	*Do you have any comments on the benefits, risks, and challenges of the use of outsourcing? Are there any additional factors which should be considered or described in the document?*

ALFI's Response to question 3

1. We rather agree with the proposed principles and measures.

2. Nevertheless we would like to share the following comments.

a. Specificities of the intra-group regime:
    a. Benefits of intragroup outsourcing are not included but come in addition to those benefits already listed: create economies of scale within the group the entity belongs to, competence/expertise remain within the group
    b. Additional Risk for intragroup outsourcing: potential conflicts of interest risk when it relates to services sourced within affiliated entities.
    c. Challenges: In a globalised world with financial conglomerates across different jurisdictions, regulated entities should be allowed to place reliance on group-wide policies and procedures on outsourcing instead of expecting local versions of the policies and procedures on outsourcing.

b. The cost element is critical to manage the value model for the end-investor.

c. Risk to make due diligence on every player, which will generate unnecessary burdensome procedures and thus additional costs for the end-investor. Due diligence should be reserved to the delegation of core functions (see. question 2).

d. With regards to the "Control" aspects, a reference to the control of the actual service provisioning seems to be missing. Regulated entities face the risk that their service provider fails to provide a service according to the service agreement (completeness, accuracy, timeliness). This creates the need for counter measures (i.e. contract design, performance evaluation, incentive structures).

e. An additional potential risk worth recognising consists in an "Exit/lock-in" risk. Existing regulations and guidance clearly require an exit plan for material (and sometimes non-material) cloud outsourcing. Sometimes exit plans however are effectively impossible, or highly unfeasible. Regulators need to acknowledge that the technology is not yet at the stage whereby it would be possible to have an instant backup of a cloud service and failover at the flick of a switch. Currently, cloud vendors have no incentive to make their services interchangeable and commoditised. On the contrary, their best interest is to make their services as unique and sticky as possible. Financial services firms are at a disadvantage here.

Chapter 3 – Fundamental precepts
F. Assessment of Materiality and Criticality

Degree of materiality or criticality

The Principles on Outsourcing set out IOSCO's expectations of regulated entities. They are written to help ensure they apply to outsourced tasks that pose risks to regulated entities and regulatory objectives.
These Principles should be applied according to the degree of materiality or criticality of the outsourced task to the ongoing business of the regulated entity and to its regulatory obligations. The Principles on Outsourcing allow for a risk-based approach to ensure they are applied to those outsourced tasks that would introduce a material or unacceptable level of risk to the entity if they were to fail or are critical to the functioning of the regulated entity or the integrity of financial markets. Even where the task is not material or critical, the regulated entity should consider the appropriateness of applying the principles as a matter of good practice.

For the purposes of CRAs in the context of these Principles, "material" or "critical" tasks include, for example, the shared use by entities within a CRA network of analytical, legal, compliance, internal controls, IT, and any other support tasks.
In understanding and applying the Principles on Outsourcing, the regulated entity should develop a process for determining the materiality or criticality of the tasks it is seeking to outsource. In simple terms, a material task is one that comprises or affects a significant proportion of the tasks of the regulated entity; a critical task may be a task that is small in scale but without which the regulated entity is unable to conduct its activities.

F. Assessment of Materiality and Criticality

Factors to be considered by the regulated entity

The assessment of what is material or critical is often subjective and depends on the circumstances of the regulated entity in question. Factors to be considered by the regulated entity may include, but are not limited to the:

- Potential risks to the regulatory objectives of maintaining fair, orderly, and transparent markets;
- Potential impact on price formation;
- Potential negative impacts on investor protection or directly on clients;
- Potential threats to relevant clearing and settlement systems;
- Whether the regulated entity would be unable to deliver core services to its clients without the relevant outsourced service;
- Financial, reputational, and operational impact on the regulated entity of the failure of a service provider to perform;
- Potential impact of a deterioration of the quality of services provided by a service provider on the regulated entity's clients;
- Potential impact on the quality of credit ratings as well as the quality of the credit rating process;
- Sensitivity of the outsourced task, such that failure to recover within a specific timeframe may pose contagion risk to the broader market;
- Potential monetary losses and other harms to a regulated entity's clients resulting from the failure of a service provider to perform;
- Impact of outsourcing the task on the ability and capacity of the regulated entity to comply with regulatory requirements and changes in requirements;
- Impact on an entity's control functions and risk management;
- Involvement of critical (including price-sensitive or client-confidential) information;
- Impact of outsourcing on the data security of the entity and clients' data integrity;
- Degree of difficulty and time required to select an alternative service provider or to bring the task in-house;

Question 4

Does the description of materiality and criticality clearly and adequately address the proportional application of these principles? If not, why not?

ALFI's Response to question 4 *(1/2)*

1. We rather agree with the proposed principles and measures.

2. Nevertheless we would like to share the following comments.

a. Rather clear for criticality, but not for materiality.

i. Distinction between materiality and criticality is vague.
ii. Method for assessing proportionality? i.e. are all criteria of equal importance?
iii. List of criteria proposed are used to assess criticality. How should materiality be assessed?
iv. Are both criticality and materiality required or does one of them suffice?
IOSCO principles on criticality and materiality should align with existing regulations (e.g. CSSF Circular 17/654 on cloud requirements) or guidelines (e.g. EBA Guidelines).

b. Affiliates (section G):

i. "… while the Principles on Outsourcing should be applied to affiliated entities where relevant, it may also be appropriate to assess and apply them with some modification",
ii. ALFI welcomes the specific section on affiliates and the intention to recognise specific risks inherent to intra-group outsourcing,
iii. However the application of the Principles on Outsourcing "with some modification" requires clarification as it is otherwise open to individual and hence non consistent approaches.

d. An aspect with regards to criticality, which could be subject to interpretation: Would delegation of transaction reporting (e.g. EMIR, SFTR) be material outsourcing, since it covers "regulatory requirements" ? However, providing compliant reporting is not essential to "running the business". It would be handy to provide for actual examples of material / non-material functions to better clarify this concept.

e. The factor listed to evaluate criticality calling "Potential impact of a deterioration of the quality of services provided by a service provider on the regulated entity's clients" would benefit a clarification. It seems the criteria is rather aimed at addressing whether the activity under assessment is client facing or has direct client impact. Quality aspects are dealt with by defining KPIs and documenting Service Level Agreements at a later stage of the outsourcing process.

ALFI's Response to question 4 *(2/2)*

f. The prior approval of sub-outsourced tasks should only concern critical tasks. Many administrative non-critical tasks are part of a critical activity (e.g. statement printing) which should be possible to sub-delegate without prior consent of the regulated entity. Imposing pre-approval of sub-contracting non-critical tasks would create unnecessary burden on every stakeholder.

g. We invite IOSCO to make the distinction between full delegation i.e. the whole regulated activity is being performed by a service provider vs partial delegation. By doing so, it would not limit the scope to the listed activities only but rather include other activities that may also pose potential outsourcing risks. These elements should be considered with reference to the response to Question 2.

Chapter 4 – Outsourcing principles

Due diligence in the selection and monitoring of a service provider and the service provider's performance

Principle 1

A regulated entity should conduct suitable due diligence processes in selecting an appropriate service provider and in monitoring its ongoing performance.

Background

It is important that regulated entities exercise due care, skill, and diligence in the selection of service providers. The regulated entity should be satisfied that the service provider has the ability and capacity to undertake the provision of the outsourced task effectively at all times.

The regulated entity should also establish appropriate processes and procedures for monitoring the performance of the service provider on an ongoing basis to ensure that it retains the ability and capacity to continue to provide the outsourced task. In determining the appropriate level of monitoring, the regulated entity should consider the materiality and criticality of the outsourced task to the ongoing business of the regulated entity and to its regulatory obligations (see Fundamental Precept E on assessment of materiality and criticality).

⇒ *See the consultation paper for the details of the proposed implementation measures.*

Question 5

Do you consider the Principle and implementation measures for due diligence are adequate and appropriate? If not, why not?

ALFI's Response to question 5

1. We rather agree with the proposed principles and measures.

2. Nevertheless we would like to share the following comments, in order to clarify the notion of Due Diligence.

a. We would recommend to make a clearer distinction between the process of due diligence and the process of implementing an ongoing monitoring of the performance of the service provider.

   For the Luxembourg market, due diligence is commonly related to the initial assessment of the service provider's capacities to provide a service AND the reoccurring re-confirmation of these capacities through regular ongoing/periodic due diligence. Ongoing monitoring has the control objective of ensuring that these capacities were actually performed by the delegate on an ongoing basis. Service level agreements and KPIs are generally used to define such performance objectives controlled in the ongoing monitoring.

b. "The appropriate level of monitoring should be determined by considering materiality or criticality of the outsourced task": more guidance would be welcome. ALFI's understanding is that criticality defines the activity to be outsourced, not the service provider which is assessed through the due diligence process.

c. Expectation of "enhanced due diligence" on cross-border outsourcing:
   a. ALFI would rather expect to see a risk-based approach applied whereby cross-border aspects are evaluated (among other criteria, see next point) rather than defining cross-border systematically as a higher risk. As a result for example, firms within EU, cross-border risk could be rated as low.
   b. In general, ALFI would expect to see a comprehensive list of criteria (including cross border) to be included in the initial due diligence and used to risk assess the service provider. The outcome of which (in combination with the criticality assessment) determines the level of ongoing due diligence required once the service provider is onboarded.

Chapter 4 – Outsourcing principles
The contract with a service provider

Principle 2

A regulated entity should enter into a legally binding written contract[5] with each service provider, the nature and detail of which should be appropriate to the materiality or criticality of the outsourced task to the business of the regulated entity.

[5] References to written contracts in this consultation report include contracts concluded by electronic means or electronic contracts stored in a durable, recordable and readable form, where permitted under the relevant law.

Background

A legally binding written contract between a regulated entity and a service provider is the critical element underpinning the relationship between the regulated entity and the service provider. Contractual provisions can reduce the risks of non-performance or aid the resolution of disagreements about the scope, nature, and quality of the service to be provided. A written contract will assist the monitoring of the outsourced tasks by the regulated entity and/or by regulators.

The level of detail of the written contract should reflect the level of monitoring, assessment, inspection and auditing required, as well as the risks, size and complexity of the outsourced services involved. In determining the nature and detail of the written contract, the regulated entity should consider the materiality and criticality of the outsourced task to the ongoing business of the regulated entity and to its regulatory obligations, as discussed in the section on assessment of materiality and criticality, above.

Where different regulatory requirements may apply for the regulated entity and the service provider due to the cross-border nature of the service, the service provider should recognise and accommodate the requirements of each jurisdiction in which it operates, as appropriate, and ensure it acts in a manner that is consistent with the regulated entity's regulatory obligations.

⇒ *See the consultation paper for the details of the proposed implementation measures.*

Question 6

Do you consider the Principle and implementation measures for establishing the contract with a service provider are adequate and appropriate? If not, why not?

ALFI's Response to question 6

We consider the principles and implementation measures adequate and appropriate.

In particular, we can see Principle 2 as a clarification / development of the current regulatory framework in force with particular reference to, among others, the Commission Delegated Regulation (EU) No 231/2013 of 19 December 2012 (Section 8 - Delegation of AIFM functions) as per articles below:

- Article 75(d) : "*the delegation arrangement takes the form of a written agreement concluded between the AIFM and the delegate*";
- Article 75(e) : "*the AIFM ensures that the delegate carries out the delegated functions effectively and in compliance with applicable law and regulatory requirements and must establish methods and procedures for reviewing on an ongoing basis the services provided by the delegate. The AIFM shall take appropriate action if it appears that the delegate cannot carry out the functions effectively or in compliance with applicable laws and regulatory requirements*";
- Article 75(f) : "*the AIFM supervises effectively the delegated functions and manages the risks associated with the delegation. For this purpose the AIFM shall have at all times the necessary expertise and resources to supervise the delegated functions. The AIFM shall set out in the agreement its right of information, inspection, admittance and access, and its instruction and monitoring rights against the delegate. The AIFM shall also ensure that the delegate properly supervises the performance of the delegated functions, and adequately manages the risks associated with the delegation".*

However, based on our past experience / lessons learnt, the implementation of Principle 2 may face some difficulties in being accepted by some market players, normally opting for standardised agreements that do not always consider the importance of a tailored fit legal framework taking into account the specific "materiality and criticality of the outsourced task to the ongoing business of the regulated entity and to its regulatory obligations". This scenario is envisaged in particular when the parent company decides to contract directly for all / most of the entities belonging to the same group.

Principle 2 shall also take into consideration the right of access to records and information for the regulatory authority of the covered entity in line with Article 79(a) of the Commission Delegated Regulation (EU) No 231/2013 of 19 December 2012.

To be also highlighted that the "EU resiliency", in the context of the cloud outsourcing, can face some technical implementation difficulties leading to the increase of related fees and associated costs.

Last and in order to facilitate the understanding and execution of the commitments, we suggest that the legal aspects of the duties be covered by a contract referring to a Service Level Agreement (SLA) defining the operational aspects.

Chapter 4 – Outsourcing principles

Information security, business resilience, continuity and disaster recovery

Principle 3

A regulated entity should take appropriate steps to ensure both the regulated entity and any service provider establish procedures and controls to protect the regulated entity's proprietary and client-related information and software and to ensure a continuity of service to the regulated entity, including a plan for disaster recovery with periodic testing of backup facilities.

Background

Effective, secure and resilient information technology systems are fundamental to the markets. IOSCO has previously stated in its Risk Outlook that potential vulnerabilities of cyber threats may arise through, inter alia, connections to unsecure vendors and the exploitation of information and communication platforms. It further emphasised that cyber threats have increased in number, sophistication and complexity over recent years.

Security breaches and cyber incidents can undermine investors' privacy and/or entities' confidentiality interests and have a damaging effect on a regulated entity's reputation, which may ultimately cause a loss of market confidence and adversely impact the overall operational risk profile of the regulated entity.

In particular, robust IT security is important where details of trade data and client assets, or the assets themselves, might be vulnerable to unauthorised access or theft. Accordingly, regulated entities should seek to ensure that service providers maintain appropriate IT security, cyber-resilience, and disaster recovery capabilities and business continuity plans. As part of its reviews of these matters, a regulated entity should also take into account whether additional issues are raised when the outsourcing is performed on a cross-border basis.

See the consultation paper for the details of the proposed implementation measures.

Question 7

Do you consider the Principle and implementation measures for information security, business continuity and disaster recovery are adequate and appropriate? If not, why not?

Question 8

What measures for business continuity would be effective in situations where all, or a significant portion, of both the outsourcers' and third-party providers' work force is working remotely? In particular what steps should be taken with respect to Cyber Security and Operational Resilience?"

ALFI's Response to questions 7 and 8

Response to Question 7
We rather agree on the concepts proposed.

Nevertheless, from a pragmatic perspective, we have identified the following key success factors for the implementation of the proposed measures:

1. Proportionality
   the bargaining power of the regulated entity will depend on its size,
2. Dialogue between the regulated entity and the service provider
   a. understanding of the offer (service providers cannot share all the details of their set-up, but only the major aspects of their policies),
   b. capacity to perform tests,
   c. capacity to negotiate clauses and specific functionalities,
   d. location of the provider (EU domiciled vs. non-EU), and the existence of an equivalence regime,
   e. concentration and dependency between the two parties.

Response to Question 8
We rather agree on the concepts proposed.

We have identified the following key success factors for the implementation of the proposed measures aimed at guaranting the integrity and security of data:

1. Specific training to raise the awareness of the risks to manipulate business data on an insecure environment,
2. Ring fencing of business tools from others (personnel), in order to avoid collusion,
3. Proper access to IT platforms, with rights granting by function (valuation, custody,…),
4. Working remotely is just a dimension of BCP contingencies. The regulated entity and the service provider have to define the terms of the remote activities.

Chapter 4 – Outsourcing principles
Confidentiality Issues

Principle 4

A regulated entity should take appropriate steps to ensure that service providers protect confidential information and data related to the regulated entity and its clients from intentional or inadvertent unauthorised disclosure to third parties.

Background

Unauthorised disclosure of confidential regulated entity or client information could have a number of negative consequences, including harm to clients and investors, damage to the regulated entity's reputation, financial losses, and the loss of or risk to proprietary information (including the regulated entity's trade secrets).

In addition, unauthorised disclosure or unauthorised access to this information could result in the intentional or inadvertent disclosure of private and sensitive information about individuals who have a reasonable expectation of privacy or a right to privacy pursuant to applicable legal provisions, and might also result in a material financial loss to an entity's clients.

In addition to the potential harm and material financial loss to a regulated entity's clients, an unauthorised disclosure could also result in the regulated entity having financial liability to its clients and/or its regulators, possibly affecting the entity's solvency.

As noted above in the discussion of concepts of outsourcing, CRAs generally do not use the terms "customers" or "clients" to refer to issuers, obligors, subscribers or investors. In the context of these Principles, for CRA's, confidential information should be understood to not just include information related to the CRA itself, but to any issuer, obligor, subscriber or investor–related information and/or software.

See the consultation paper for the details of the proposed implementation measures.

Question 9

Do you consider the Principle and implementation measures for the management of confidentiality issues are adequate and appropriate? If not, why not?

ALFI's Response to question 9

We consider the principles and implementation measures adequate and appropriate.

In particular, we can see Principle 4 as a clarification / development of the current regulatory framework in force with particular reference to, among others, the Commission Delegated Regulation (EU) No 231/2013 of 19 December 2012 (Section 8 - Delegation of AIFM functions) as per article below:

- Article 75(k) : "*the AIFM ensures that the delegate protects any confidential information relating to the AIFM, the AIF affected by the delegation and the investors in that AIF".*

We understand that Principle 4, in line with the above listed article of the Commission Delegated Regulation (EU) No 231/2013 of 19 December 2012, requests regulated entities their best effort in this respect.

Chapter 4 – Outsourcing principles
Concentration of outsourcing arrangements

Principle 5

A regulated entity should be aware of the risks posed, and should manage them effectively, where it is dependent on a single service provider for material or critical outsourced tasks or where it is aware that one service provider provides material or critical outsourcing services to multiple regulated entities including itself.

Background

Concentration risks may arise when one regulated entity relies extensively on one service provider or when many regulated entities rely on one or very few service providers.
Where multiple regulated entities use a common service provider, operational risks are correspondingly concentrated, and may pose a threat of systemic risk.

* For example, if the service provider suddenly and unexpectedly becomes unable to perform services that are material or critical to the business of a significant number of regulated entities, each of the regulated entities will be similarly disabled.
* Alternatively, if multiple regulated entities depend upon the same provider of business continuity services (e.g., a common disaster recovery site), a disruption that affects a large number of those entities may result in a lack of capacity for the business continuity services.

Either of these scenarios may result in negative effects on markets that depend on participation by the impacted regulated entities, or more generally on public confidence in the functioning of financial markets.
Similarly, where a regulated entity is significantly dependent on a single service provider for the provision of outsourced tasks, a concentration risk exists. This may result in business continuity concerns should an interruption to the provision of tasks occur. Where the regulated entity is critical to a particular market, service or asset class this may also increase systemic risk.
It is recognised that a single regulated entity, despite using best endeavours, may not be aware of, or have enough information to assess, situations where one service provider provides outsourcing services to multiple regulated entities.

See the consultation paper for the details of the proposed implementation measures.

Question 10

Do you consider the Principle and implementation measures for the management of concentration risk in outsourcing arrangements are adequate and appropriate? If not, why not?

ALFI's Response to question 10

1. We rather agree with the proposed principles and measures.

2. Nevertheless we would like to share the following comments.

    - ALFI would welcome a distinction being made between (i) Firm-specific concentration (i.e. a regulated entity relying too much on the services of a single service provider) and (ii) Industry-wide concentration,
    - ALFI agrees that Firm specific concentration risk is a responsibility of the regulated entity to identify, manage and risk accept, develop exit strategies,
    - IOSCO however seem to expect regulated entities to also manage Industry wide concentration risks which does not seem realistic. This model may put industry participants at a competitive disadvantage, which in turn might not be in the best interest of investors (i.e. having to opt for another service provider less competitive because of an industry concentration risk on the preferred service provider),
    - Additionally, ALFI would welcome more guidance, eventually in the form of templates, for how outsourcing to dominant market players should be contractually documented.

Chapter 4 – Outsourcing principles

Access to data, premises, personnel and associated rights of inspection.

Principle 6

A regulated entity should take appropriate steps to ensure that its regulator, its auditors, and itself are able to obtain promptly, upon request, information concerning outsourced tasks that is relevant to contractual compliance and/or regulatory oversight including, as necessary, access to the data, IT systems, premises and personnel of service providers relating to the outsourced tasks.

Background

Regulated entities should ensure that their regulator has prompt and comprehensive access, inspection, investigation and monitoring powers over the activities for which they are regulated. Generally, the scope of supervision should not be impacted by a regulated entity's decision to engage a service provider. The regulated entity retains full responsibility, legal liability and accountability to the regulator for all tasks that the regulated entity may outsource to a service provider to the same extent as if the service were provided in-house.

Accordingly, regulated entities should make provision in their arrangements with service providers for prompt access by regulators to relevant premises that relate to the provision of services to the regulated entity, and to key personnel who manage and oversee the outsourced services.

Regulated entities should ensure that their regulators should also be able, upon request, to obtain promptly any data relating to or generated by the outsourced task, irrespective of whether they are in the possession of the regulated entity or the service provider and to obtain any additional information concerning the tasks performed by the service provider.

A regulator's access to such data may be direct or indirect (depending on regulatory requirements), although the regulated entity should always maintain its own direct access to such data. The regulated entity may be required by its regulator to ensure that data is maintained in the regulator's jurisdiction, such as through a locally stored back-up of relevant data, or that the service provider will provide originals or copies of the data to the regulator's jurisdiction upon request.

To facilitate the regulator's prompt access and to maintain orderly business operations of the regulated entities, arrangements between regulated entities and service providers should seek to ensure that the regulated entities, its auditors and regulators have appropriate prompt access to the premises, personnel, and data and other information where it is held.

Such access to data should be in a form that is acceptable to the regulator. This should be considered in terms of both the format in which information is made available (e.g. electronic versus paper) and the language in which the material is provided, particularly where the outsourced task is performed in a jurisdiction other than that of the regulated entity.

See the consultation paper for the details of the proposed implementation measures.

Question 11

Do you consider the Principle and implementation measures for ensuring access arrangements are adequate and appropriate? If not, why not?

ALFI's Response to question 11

We believe that the Principles and implementation measures for ensuring access arrangements are adequate and appropriate from a theoretical perspective, albeit not always feasible from a practical point of view.

The negotiation reality/balance of contracting with a much larger provider (e.g. a lead cloud services provider) is such that the service provider may not be willing to accept terms in relation to physical on-site visits unless this is required/authorised by local regulators. In addition, data protection considerations shall be taken into account according to local requirements.

We agree with IOSCO on having terms related to exit strategies, however we do not think it would be acceptable that in case of contract termination the supervisor(s) of the regulated entities should continue to have access to proprietary data and systems of the service providers. The entity should be able to repatriate books, records and information to allow the regulator to continue having access to them.

Chapter 4 – Outsourcing principles
Termination of outsourcing arrangements

Principle 7

A regulated entity should include written provisions relating to the termination of outsourced tasks in its contract with service providers and ensure that it maintains appropriate exit strategies.

Background

Where a task is outsourced, there is an increased risk that the continuity of the particular task in terms of daily management and control of that task, related information and data, staff training, and knowledge management, is dependent on the service provider continuing in that role and performing that task. This risk should be addressed by an agreement between the entity and the service provider taking into account factors such as when an outsourcing arrangement can be terminated, what will occur on termination and strategies for managing the transfer of the task back to the entity or to another party.

There should be clarity on who owns the relevant data, and whether the service provider has any retention rights.

The written contract and exit strategies should be viewed as separate concepts, though there may be aspects of an exit strategy included in a written contract e.g. an undertaking that the service provider cooperates with the firm to manage the exit when the firm decides to leave the service provider.

See the consultation paper for the details of the proposed implementation measures.

Question 12

Do you consider the Principle and implementation measures for the termination of outsourcing arrangements are adequate and appropriate? If not, why not?

Question 13

Do you have any other comments on the Principles and implementation measures? Do you have any suggestions for other areas or risks IOSCO should address?

ALFI's Response to question 12

We consider the principles and implementation measures adequate and appropriate.

In particular, we can see Principle 7 as a clarification / development of the current regulatory framework in force with particular reference to, among others, the Commission Delegated Regulation (EU) No 231/2013 of 19 December 2012 (Section 8 - Delegation of AIFM functions) as per articles below:

- Article 75(g) : "*the AIFM ensures that the continuity and quality of the delegated functions or of the delegated task of carrying out functions are maintained also in the event of termination of the delegation either by transferring the delegated functions or the delegated task of carrying out functions to another third party or by performing them itself";*
- Article 75(h) : "*the respective rights and obligations of the AIFM and the delegate are clearly allocated and set out in the agreement. In particular, the AIFM shall contractually ensure its instruction and termination rights, its rights of information, and its right to inspections and access to books and premises. The agreement shall make sure that sub-delegation can take place only with the consent of the AIFM".*

However, based on our past experience / lessons learnt, the implementation of Principle 7 may face some difficulties in being accepted by some market players.

In particular, the obligation of the service provider to assist and provide full support for a successful and complete transition to another service provider may be subject to discussion / negotiation between the different parties, with particular reference to the relevant tasks ownerships and associated costs to be fully clarified and agreed at the beginning of the relationship, and that shall take into consideration also the (potential) future business development of the financial entities and of the relevant business relationships.

In addition, a clear delineation of ownership covering intellectual property following the contract's termination may be difficult to be agreed and implemented in a contract taking into consideration the legal requirements in the country of establishment of the service provider.

ALFI's Response to question 13

We are of the view that the following points should be taken into account in order to facilitate an effective implementation of the principles proposed in the consultation:

1. In light of the response to Question 2, we believe each of the concepts of Outsourcing and Delegation should be subject to distinct definitions. This would clarify typology of functions and activities coverage. It is worth noting that the concept of Delegation as defined in the AIFMD and UCITS V directive is already broadly used and applicable within the asset management industry.

2. A reference to the equivalence regime would facilitate the identification of jurisdictions benefiting from a regulatory framework akin to the EU's. Outsourcing and Delegation are already regulated very strictly within the EU and towards third countries subject to the same standards, procedures and conditions in order to ensure uniform client / investor protection.

ALFI welcomes this opportunity to respond to IOSCO's consultation on outsourcing principles and implementation measures and looks forward to collaborating further with the Committees.