FSB FINANCIAL STABILITY BOARD

# Feasibility study on approaches to aggregate OTC derivatives data

**19 September 2014**

**Contents** **Page**


Executive Summary ..... 1

Introduction ..... 3

1. Objectives, Scope and Approach ..... 5

**1.1** Objectives and Scope of the Study ..... 5

**1.2** Aggregation Models Analysed ..... 5

**1.3** Preparation of the Study ..... 8

**1.4** Definition of Data Aggregation ..... 8

**1.5** Assumptions ..... 9

**2.** Stocktake of Existing Trade Reporting ..... 10

**2.1** TR reporting implementation and current use of data ..... 10

**2.2** Available data fields and data gaps ..... 11

**2.3** Data standards and format ..... 12

**2.4** Legal and privacy issues ..... 12

**3.** Authorities' Requirements for Aggregated OTC Derivatives Data ..... 13

**3.1** Data Needs ..... 13

**3.2** Aggregation Minimum Prerequisites ..... 14

**3.3** Further aggregation requirements ..... 16

**4.** Legal Considerations ..... 20

**4.1** Types of existing legal obstacles to submit/collect data from TRs into an aggregation mechanism ..... 21

**4.2** Legal challenges to access to TR data ..... 24

**4.3** Legal considerations for the governance of the system ..... 25

**5.** Data & Technology Considerations ..... 31

**5.1** The Impact of the Aggregation Option on Data and Technology ..... 31

**5.2** Data aggregation and reporting framework ..... 31

**5.3** Principles of data management to facilitate proper data aggregation ..... 35

**6.** Assessment of Data Aggregation Options ..... 41

**6.1** Criteria used for the Assessment ..... 42

**6.2** Assessment of varying degrees of comprehensiveness of service in the implementation of Options 1 and 2 ..... 49

**6.3** Cost drivers and other cost considerations ..... 55

Appendix 1: Terms of reference for feasibility study ..... 58
Appendix 2: Data quality dimensions ..... 66
Appendix 3: Extract from Table 6.2 of the Access Report ..... 69
Appendix 4: Data elements ..... 72
Appendix 5: Summary of the outreach workshop ..... 74
Appendix 6: Working Group participants ..... 85
Appendix 7: Glossary of abbreviations ..... 89
Appendix 8: List of references ..... 91

## Executive Summary

G20 Leaders agreed in 2009 that all over-the-counter (OTC) derivatives contracts should be reported to trade repositories (TRs), as part of their commitments to reform OTC derivatives markets in order to improve transparency, mitigate systemic risk and protect against market abuse. To date, a total of 25 TRs in 11 jurisdictions are either operational or have announced that they will be, and these numbers may increase. Aggregation of the data being reported across these TRs is necessary to ensure that authorities are able to obtain a comprehensive global view of the OTC derivatives market and activity. The FSB therefore requested a study of the feasibility of various options for a mechanism to produce and share global aggregated data. The feasibility study should take into account legal and technical issues and the aggregated TR data that authorities need to fulfil their mandates. This study responds to that request.

A consultative version of this report (without recommendations at that stage) was published on 4 February 2014. The public feedback received has been taken into account in this report.[1]

As mandated by the FSB, this report compares three basic options for aggregating TR data: Option 1 is a physically centralised aggregation mechanism; Option 2 is a logically centralised aggregation mechanism; and Option 3 involves the collection of raw data from individual TR databases by individual authorities that then aggregate the data themselves within their own systems.

The options are compared according to their suitability for meeting authorities' needs as data users, and the legal, data and technology considerations that they give rise to.

This report finds that aggregation Options 1 and 2 are highly preferable to Option 3 in order to ensure that authorities have access to the aggregated data that they need in order to perform their mandates and meet the G20 objectives. While Option 3 is the only one of these options that is currently available for use, it has practical limitations that allow it to meet only part of authorities' data needs, beyond protecting against market abuse. However, this study has not arrived at a preference between Option 1 and 2. On the one hand, Option 1 would require a large expandable central data storage and computation facility, and the data would only be as timely as the latest run of the data loading cycle. On the other hand, Option 2 would require the individual TRs to host additional technology that would link the central aggregator to their respective databases, and there would be short delays in retrieving data compared to querying a pre-loaded database. Even if Options 1 or 2 were chosen, Option 3 will continue to be an additional option available for individual authorities to pursue (based on their requirements) to supplement their use of Option 1 or 2.

The study finds that there are important issues to address alongside whether the aggregation model should be physically centralised or logically centralised. These questions include the need for greater standardisation of data reported to TRs and amending laws and regulations to allow a centralised aggregation mechanism to access TR data. Indeed, Options 1 and 2 share

[1] The public feedback is available on the FSB website at http://www.financialstabilityboard.org/publications/c_140416.htm.

many legal, data and technology features and requirements, rather than representing fundamentally different approaches.

The report outlines key steps that would be needed to undertake either Option 1 or Option 2. Amongst these steps, it is critical for any aggregation option that the work on standardisation and harmonisation of important data elements be completed, including in particular through the global introduction of the Legal Entity Identifier (LEI), and the creation of a Unique Transaction Identifier (UTI) and Unique Product Identifier (UPI). The report also indicates, in broad terms, the types of legal and regulatory changes that would be needed to allow a central mechanism to aggregate data for authorities. While further work in both these areas will be challenging globally, they are essential for a central aggregation mechanism to be effective.

Options 1 and 2 could be implemented to varying degrees of comprehensiveness of service to data users, along various dimensions, including: the depth of the data maintained, the breadth of the data maintained, information on the identity of the counterparty, the asset classes covered, and the degree of data manipulation performed by the aggregator. (These five dimensions are defined further in Chapter 1.) The less comprehensive versions along these dimensions may constrain the ability of authorities to conduct the overall range of tasks under their financial stability, supervisory and regulatory mandates while reducing only to a limited extent the legal, data and technological challenges to implementing the options. In this regard, such versions could be considered as a first step of a phased approach until the fully comprehensive versions of the aggregation options are able to be implemented. In the interim, authorities may need to rely on data obtained directly from TRs (in effect, Option 3) to meet some elements of their mandates (notwithstanding the above-mentioned limitations of this option). To this end, work underway to develop bilateral memoranda of understanding (MoUs) between authorities should continue until a central aggregation mechanism can be implemented.

In addition to the discussion of aggregation options, the report also discusses: (a) the data needs the aggregation mechanism should be designed to meet, (b) the legal and governance aspects that would need to be addressed in setting up the mechanism, and (c) the data and technology aspects, including key drivers of costs, data elements needed, and principles of sound data management to achieve high quality data aggregation.

The report does not attempt to analyse the specific technological choices of hardware and software, or define the specific legal and governance requirements. At this early stage of the analysis of the options, with so many elements of the scope and scale of the exercise still undefined, it is difficult to estimate accurately the costs of the different options. Based on a very preliminary and qualitative cost-driver analysis conducted by the group, this report estimates that options 1 and 2 would have similar costs, although they would be distributed in different ways. Though no central system is required under Option 3, this option is likely to be globally more expensive than either Option 1 or Option 2 when the final costs borne by individual regulators and TRs are taken into account.

As next steps, this report recommends the following, which will be needed irrespective of the particular aggregation model chosen.

- The work to establish uniform global identifiers, i.e. agreement on a UTI and UPI as well as adoption of the LEI, should be accelerated to ensure that OTC derivatives data can be adequately aggregated. These steps are important under any option for an

aggregation mechanism, and indeed more generally to improve the usability of TR data. The work will probably require official sector impetus and coordination as well as partnership with the industry to achieve global acceptance and serve public interest goals.

- International work should take place, involving a broad range of authorities and TRs, to develop global guidance on harmonisation of data elements that are reported to TRs and are important to aggregation by authorities.
- The work to develop and implement a global aggregation mechanism should not wait until the global identifiers are in place. If policy-makers decide to develop such a mechanism, that work should be conducted in parallel with the development of identifiers to ensure that the global aggregation of data can be implemented as soon as possible to enable authorities to fulfil their mandates.
- As part of the work leading to the implementation of the global aggregation mechanism, and before any formal project is launched, the following steps should be urgently undertaken:
    - Study in more detail and address the legal and regulatory changes that would be needed to implement a global aggregation mechanism that would meet the range of authorities' data access needs;
    - Further consider the appropriate governance structure of an aggregation mechanism;
    - Study further the data and technological requirements for an aggregation mechanism so as to better support a more detailed project specification.
    - Undertake a more detailed assessment of potential costs, beyond the initial discussion of cost drivers provided in this report, based on further analysis of the business requirements and priorities of the authorities and complexity of the use cases.

These steps are critical to putting authorities in position to launch a project to develop a global aggregation mechanism, should they decide to do so.

## Introduction

G20 Leaders agreed, as part of their commitments regarding OTC derivatives reforms, that all OTC derivatives contracts should be reported to TRs. They also asked the FSB and its members to assess whether implementation of these reforms is sufficient to improve transparency in the derivatives markets, mitigate systemic risk, and protect against market abuse.

A good deal of progress has been made in establishing the TR infrastructure to support the commitment that all contracts be reported. Currently, multiple TRs operate, or are undergoing approval processes to do so, in a number of different jurisdictions. The requirements for trade reporting differ across jurisdictions and TRs differ in their practices. The result is that TR data are fragmented across many locations, stored in a variety of formats, and subject to many different rules for authorities' access. The data in these TRs will need to be aggregated in various ways if authorities are to obtain a comprehensive and accurate view of the global

OTC derivatives markets and to meet the original financial stability objectives of the G20 in calling for comprehensive use of TRs.

The FSB, CPSS and IOSCO have identified the need for further study of how to ensure that the data reported to TRs can be effectively used by authorities, including identifying and mitigating systemic risk, and in particular through enabling the availability of the data in aggregated form. The FSB set up a group – the Aggregation Feasibility Study Group (AFSG) – to study the feasibility of several options to produce and share global aggregated TR data, taking into account legal and technical issues and the types of aggregated data that authorities need to fulfil their mandates and to monitor financial stability. The FSB's terms of reference for the study are attached as Appendix 1.

This report takes as a starting point existing international guidance and recommendations relating to TRs, including those contained in the January 2012 CPSS-IOSCO report on OTC derivatives data reporting and aggregation requirements ("Data Report") and the August 2013 CPSS-IOSCO report on authorities' access to TR data ("Access Report"). It has also made use of the semi-annual FSB progress reports on the implementation of OTC derivatives market reforms, including on the implementation of comprehensive trade reporting requirements.

**Structure of the Report**

The report is structured as follows.

**Chapter 1** lays out the objectives, scope and approach followed by the feasibility study, and describes the three broad options for aggregation that the study assesses.

**Chapter 2** makes a brief stocktake of the current status of implementation of reporting to TRs, including the current and planned global configuration of TRs, in order to provide background on the scale and scope of the aggregation challenges.

**Chapter 3** summarises the different types of requirements of authorities for aggregated OTC derivatives data, focusing in particular on the minimum prerequisites for aggregation so that the data are useable by authorities to fulfil their various mandates.

**Chapter 4** describes the legal and policy considerations, concerning submission of data, access to data and governance of the aggregation mechanism, which are relevant to the choice of aggregation model.

**Chapter 5** discusses the data and technology considerations associated with meeting authorities' requirements for aggregated data under the different choices of model.

**Chapter 6** presents the criteria for the assessment of the options derived from the discussion in Chapters 3, 4 and 5, and the assessment of the pros and cons of the different aggregation options against those criteria. This chapter assesses the implications of different levels of comprehensiveness of service that could be provided by the aggregation mechanism, focusing for illustrative purposes on three different "use cases" for how authorities would aim to use aggregated data to achieve their mandates. The chapter also includes a preliminary analysis of the various drivers of costs in setting up and operating an aggregation mechanism.

# 1. Objectives, Scope and Approach

## 1.1 Objectives and Scope of the Study

The goal of this feasibility study is to set out and analyse the various broad options for aggregating TR data for use by authorities in effectively meeting their respective mandates. The FSB, in consultation with CPSS and IOSCO, will subsequently make a decision on whether to initiate work to develop a global aggregation mechanism and, if so, according to which type of aggregation model and which additional policy actions are needed to address obstacles.

The report is structured to provide the relevant information for senior policy-makers to be able to make the above decisions, and to inform both senior policy-makers and the public about the analysis supporting that information.

The study is intentionally high-level in approach, comparing the effectiveness of the broad types of options that could be used in meeting the G20 goal that authorities are able to have a global view of the OTC derivatives markets. It does not attempt to analyse the specific technological choices of hardware and software, or define the specific legal and governance requirements. At this early stage of the analysis of the options, with so many elements of the scope and scale of the exercise still undefined, it is not possible to estimate the costs of the different options. The report includes instead a qualitative analysis of the relative complexity of the different options and a broad analysis of the main factors that would drive costs. More detailed work on such issues is expected to take place in any follow-on work that may be commissioned by policy-makers.

## 1.2 Aggregation Models Analysed

The main options for aggregating TR data explored by this study are:

**Option 1. A physically centralised model of aggregation.** This model would feature a central database where required data on transactions and (if needed and available) on positions and collateral would be collected from TRs and stored on a regular basis. The facility housing the database would provide services to report aggregated data to authorities, drawing on the stored underlying transaction, position and collateral details. In order to do so, the facility would perform functions such as data quality checks, removing duplications, and masking or anonymising data as needed.[2] Reports and underlying data would be available to authorities as needed and permitted according to individual authorities' access rights.

**Option 2. A logically centralised model of aggregation.** This model would feature federated (physically decentralised) data collection and storage of the same types of data as in Option 1. It would not physically collect or store data from TRs (other than temporary local caching where necessary in the aggregation process). Instead it would rely on a central logical catalogue/index to identify the location of data resident in the TRs, which would assist individual authorities in obtaining data as needed and permitted under their access rights. In this model, the underlying data would remain in local TR databases and be aggregated via logical centralisation by the aggregation mechanism, being retrieved on an "as needed" basis at the time the aggregation program is run.[3]

---

[2] Alternatively, some of these functions may already have been performed by the TR before delivering the data to the facility.

[3] Within Option 2, data standardisation and harmonisation can be performed at a centralised or at a decentralised level. Such sub-options do not fundamentally impact the following analysis and discussion.

**Option 3. Collection of raw data from local TR databases by individual authorities that then aggregate the data themselves within their own systems.** Under this option, there would be no central database or catalogue/index. All the functions of access rights verification, quality checks, etc., would be performed by the requesting authority and the responding authorities or TRs on a case-by-case basis. Access would be granted based on the rules and legislation applicable to each individual TR. In many ways, Option 3 represents the current situation for authorities wishing to aggregate data (albeit without a global set of arrangements in place for users to access all the data they need). As noted later in this report, truly global and comprehensive data aggregation is not possible under current arrangements as no individual authority or body has comprehensive access to all data in all TRs. Under Option 3, authorities could expand their cross-border access to data from current levels by concluding additional international (probably bilateral) agreements, but the absence of a centralised aggregation mechanism would seem to preclude the provision of some forms of aggregated data, notably anonymised counterparty-level data aggregated across multiple TRs.

***Differing versions of comprehensiveness of service to users***

Either Option 1 or Option 2 could be implemented with varying degrees of comprehensiveness of service level, along various dimensions including:

- ***the depth of the data maintained***: whether data is maintained at the level of individual transactions, bilateral individual positions between each pair of counterparties, or instead at aggregate level summed according to various categories.
- ***the breadth of the data maintained***: whether data is maintained covering all counterparties or instead only a predetermined set of counterparties.
- ***the identity of the counterparty***: whether the aggregator is able to provide authorities with data on named individual counterparties or only anonymised data.
- ***the asset classes covered***: whether the aggregator covers all asset classes or only some asset classes.
- ***the degree of manipulation by the aggregator***: whether the central aggregator offers only basic functionalities – such as serving as a simple pass-through of data from TRs to authorities – or more comprehensive functionalities for manipulating and reporting data.

For any aggregation mechanism a version with an initially less comprehensive service level must be able to be converted to provide more comprehensive functionality in a phased approach over time. In other words, the mechanism must be scalable in terms of the service it provides.

The less comprehensive versions of Options 1 and 2 may be less complex to implement but would not deliver the full range of services or meet the full range of uses of data that authorities need in order to meet their mandates. Chapter 6 of this report includes an evaluation of the extent to which less comprehensive versions of each option could meet the range of user requirements and their pros and cons in terms of legal, data and technology considerations. It should also be noted that decreasing the level of service provided by the central aggregator may have the effect of shifting the complexity to other parts of the overall aggregation process (e.g. either to the TRs or to the user authorities) and may not necessarily reduce the complexity of the overall process of authorities obtaining access to aggregated data.

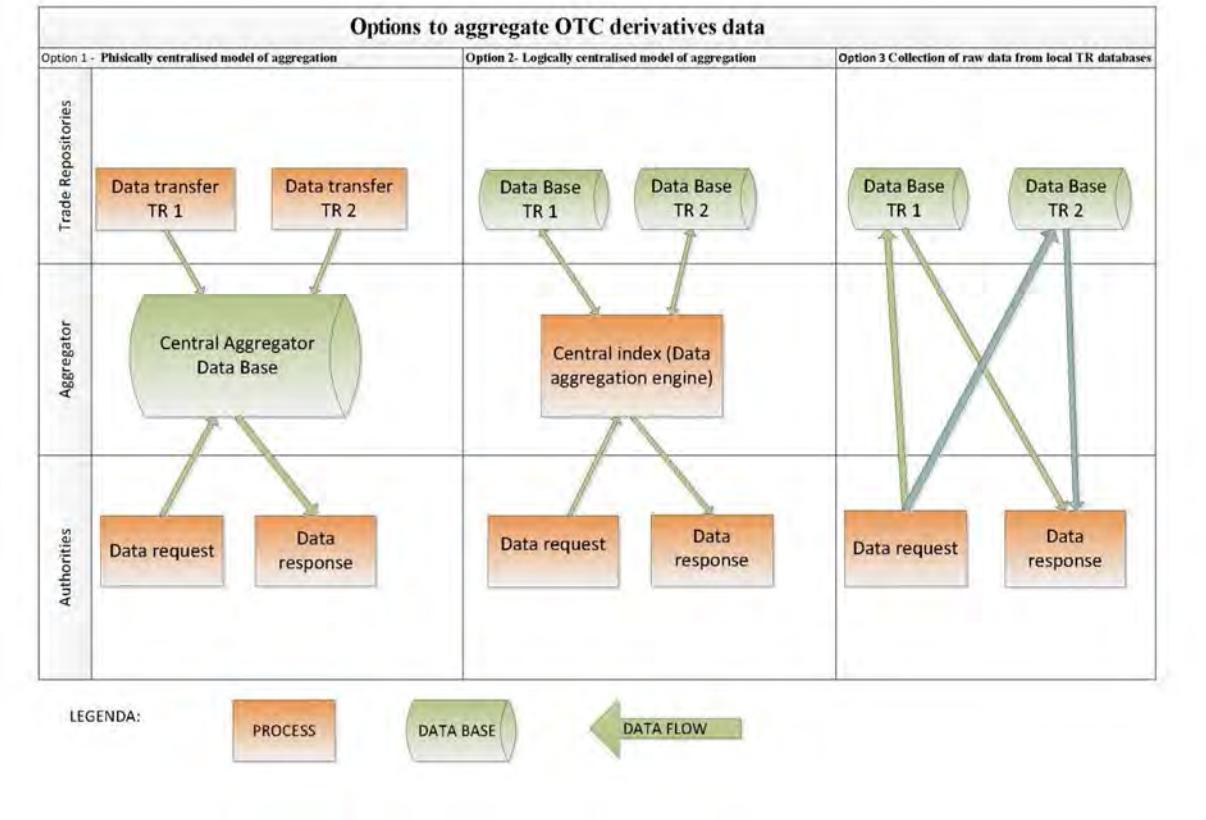
***Terminology***

In this report, the term "aggregation model" is used to refer to any one of the three Options 1, 2 or 3 above. The term "aggregation mechanism" refers to mechanisms modelled on Option 1 and Option 2 as described above, while the term "central aggregator" refers to the central data base (under Option 1) or central index and aggregation engine (under Option 2) through which the aggregation mechanism operates. The term "option" is used to refer to each of the three Options 1, 2 or 3, whereas "version" is used to refer to the different versions of comprehensiveness of service that could be provided under either Option 1 or 2 as described above.

***Summary representation of options***

The table below summarises the division of roles under the different aggregation models in performing the main tasks involved in aggregation, and the accompanying diagram provides a visual representation.

| | **Option 1: A physically centralised model of aggregation** | **Option 2: A logically centralised model of aggregation** | **Option 3: Collection of raw data from local TR databases by individual authorities that then aggregate the data themselves within their own systems** |
|---|---|---|---|
| **Storage of data used in aggregation** | Centralised storage within aggregation mechanism | TRs for underlying data<br>Temporary storage in aggregation mechanism | TRs |
| **Quality checks / removing duplication** | Aggregation mechanism or receiving authorities, depending on the comprehensiveness of the services to be provided by the aggregation mechanism | Aggregation mechanism or receiving authorities, depending on the comprehensiveness of the services to be provided by the aggregation mechanism | Receiving authorities |
| **Masking/ anonymising data if required** | Aggregation mechanism or TRs, depending on the comprehensiveness of the services to be provided by the aggregation mechanism | Aggregation mechanism or TRs, depending on the comprehensiveness of the services to be provided by the aggregation mechanism | TRs or home authorities of TRs |
| **Data delivery to authorities** | Aggregation mechanism | Aggregation mechanism | TRs or home authorities of TRs |




## 1.3 Preparation of the Study

The design of the study, including the diverse expertise within the AFSG, public consultation on the draft report and publication of the final report, is intended to ensure that the policy-makers have the benefit of a wide range of input before deciding upon the next steps, including which option to pursue.

In preparing the report the AFSG has used a variety of sources, including:

- existing reports and studies (see full list of references in Appendix 10);
- a survey of authorities in FSB member jurisdictions to gather additional information on the OTC derivatives data currently reported to TRs and accessed by authorities, as well as the status of their data aggregation capabilities on both jurisdictional and global levels;
- a workshop to discuss technical and legal issues in relation to the implementation of the alternative options, bringing together members of the AFSG and experts in the data, IT and legal issues involved from inside and outside the financial industry (see Appendix 2);
- feedback received from the public consultation process.

## 1.4 Definition of Data Aggregation

This report uses the Data Report definition of data aggregation "as the organisation of data for a particular purpose, i.e., the compilation of data based on one or more criteria". Data aggregation may or may not involve logical or mathematical operations such as summing, filtering and comparing.

As noted in the Access Report, authorities (depending on their mandates) may require access to aggregated data:

- at three levels of depth:
    1. Transaction-level (data specific to uniquely identified market participants and transactions)
    2. Position-level (gross or netted open positions specific to a uniquely identified participant or pair of participants)
    3. Aggregate-level (summed data according to various categories, e.g. by product, maturity, currency, geographical region, type of counterparty, underlier, that are not specific to any uniquely identifiable participant or transaction)
- according to a certain level of breadth (in terms of scope of participants and products/underliers), and
- according to a certain level of identity (named versus anonymous).[4]

An important distinction in terminology therefore exists between the terms "aggregated data" and "aggregate-level data". "Aggregated data" are data that have been collected together, but may or may not have been summed; the data could instead be available at transaction-level or position-level. This process of collecting the data together is referred to as "data aggregation". "Aggregate-level" data, on the other hand, are data that have been summed according to a certain categorisation so that the data no longer refer to uniquely identifiable transactions.

Different authorities (or the same authority at different times) will require access at different levels of depth, breadth and identity for different purposes. The aggregation mechanism will need to be flexible enough to provide authorities with the level of access that they require and are entitled to for these different purposes (consistent with the comprehensiveness of service that the mechanism has been designed to provide). Chapter 3 discusses these data needs and how they affect aggregation requirements in more detail.

## 1.5 Assumptions

The study focuses on the feasibility of options for data aggregation in the current regulatory and technological environment and given the existing (and planned) global configuration of TRs. In particular, the study is based on the following assumptions:

- that comprehensive reporting of OTC derivatives trades is achieved in the major jurisdictions, in accordance with the G20 commitment;
- that TRs operate under their existing functionality and data collection practices;
- that the aggregation option being considered would complement, rather than replace, the existing operations of TRs and authorities' existing direct access to TR data.

The study does not set out to propose changes to the data reported to TRs or the data held by TRs unless those changes are necessary or desirable to achieve aggregation. However, where

[4] More detail on the concepts of depth, breadth and identity is available in the Access Report.

needed, the study highlights any regulatory or other actions that might be needed in order to enable an option to be implemented or to improve its effectiveness. It notes where relevant improvements in market practices or infrastructure – e.g., introduction of a global UPI and UTI – that would assist the aggregation process, and it recognises where relevant that the aggregation option chosen may have impacts on TRs, market participants, related data providers, authorities and other stakeholders.

# 2. Stocktake of Existing Trade Reporting

## 2.1 TR reporting implementation and current use of data

As indicated in the FSB's seventh progress report on the implementation of OTC derivatives market reforms,[5] a total of 25 TRs in 11 jurisdictions are either operational or have announced that they will be. It is not anticipated that TRs will be located in all jurisdictions but rather that regulatory frameworks will, in some instances, facilitate reporting of market participants' transactions to foreign-domiciled TRs that are recognised, registered or licensed locally. The jurisdictional coverage of TRs has expanded in recent months. The majority (13) of FSB member jurisdictions now have at least one TR available to receive transaction reports, whether located domestically or operating across borders. This increase in availability in part reflects jurisdictional progress in bringing into effect in recent months regimes to permit TR operation and to require reporting. A number of other jurisdictions' regimes are expected to come into effect over the course of 2014, which should see availability increase further. Currently, in any given jurisdiction, the number of TRs eligible for reporting ranges from zero to 11, and foreign TRs from zero to eight.

The pace of implementation of TR reporting shows some differences across jurisdictions. In several jurisdictions there is some form of phased implementation, whether by asset classes or by market participant categories (largest financial participants/below threshold, regulated/end user). By end-2014, a significant number of jurisdictions will have mandatory TR reporting in place for all asset classes. Other jurisdictions are either expected to have mandatory TR reporting in place by 2015 or have not yet set a date for all asset classes.

The scope of implementation presents some differences. For instance, while financial institutions are subject to reporting in all jurisdictions, in some jurisdictions non-financial institutions may not be subject to mandatory reporting or some thresholds may be in place. In some jurisdictions, transactions have to be conducted and booked locally in order to be subject to reporting, while in other jurisdictions transactions conducted locally but not booked locally or not conducted locally but booked locally are also subject to reporting. In some jurisdictions two-sided reporting is required while other jurisdictions have opted for one-sided reporting.

In all but one jurisdiction[6], reporting has to be made to TRs, with reporting to authorities being only a fall-back option when there is no TR in place.

---

[5] See FSB April 2014 progress report on implementation of OTC derivatives market reforms: http://www.financialstabilityboard.org/publications/r_140408.pdf.

[6] In that jurisdiction, reporting to either the TR or authorities is allowed.

The time limit for reporting may also vary across jurisdictions from reporting on the same day, up to T+30, with most jurisdictions applying a reporting limit under T+3.

In most jurisdictions where TR reporting requirements are in place, authorities have access to the data held in the TRs that is consistent with their mandates. However in some jurisdictions, only a subset of authorities has regulatory access based on the current regulation in place. In other jurisdictions, where TR reporting requirements are not yet in place, access is provided on a voluntary basis. These differences reflect the different pace of TR legislation implementation across jurisdictions.

Authorities usually receive the data based on a specific format according to their respective mandate (with the format differing across authorities) while in some jurisdictions authorities have continuous online access to TRs. Most authorities have access to data based on several mandates (such as financial stability assessment, micro-prudential supervision and market surveillance and enforcement).

Even once reporting requirements are in place in all jurisdictions, no single authority or body will have a truly global view of the OTC derivatives market, even on an anonymised or aggregate-level basis, unless a global aggregation mechanism is developed. Only a global aggregation mechanism can therefore provide a practical way for all authorities to meet the minimum level of access that they would typically require in support of their mandates and responsibilities, as described in the Access Report.

## 2.2 Available data fields and data gaps

The review of data collected by TRs demonstrates that there are strong commonalities in the data fields collected across jurisdictions for a number of key economic terms of contracts such as start dates, description of the payment streams of each counterparty, face value, option information on options (needed to model value), and execution information such as execution venue name and type. However, some differences in approach remain, for instance:

- the main difference is that data on exposures (e.g. market value of transactions and collateral or margining information) are mandated for reporting in some jurisdictions, while they are not in other jurisdictions,
- the distinction between standardised and bespoke contracts is reported only in one jurisdiction,
- execution information is widely reported except the information on whether a trade is price-forming[7], which is collected only in a few jurisdictions,
- central clearing information is not widely reported, with the name of the CCP being collected only in a few jurisdictions. In some jurisdictions, transactions once cleared must be reported as being modified transactions, while in other jurisdictions, the clearing results in the required reporting of both the termination of the initial transaction and the initiation of new ones.

[7] A price-forming trade is a transaction negotiated at open market prices between two counterparties; non-price-forming trades are administrative trades entered into, e.g. to assign risk to another legal entity (e.g. to a CCP) or for scheduled compressions,

While transaction, product and counterparty identifiers are widely used, it seems that transaction and product identifiers may depend on different taxonomies which would require further details to ensure unicity (for transaction identifiers) and to check for consistency (for product identifiers) before aggregation.

## 2.3 Data standards and format

The review of data standards and formats used by the different TRs in collection and storage of OTC derivatives data demonstrates that different approaches were chosen by various jurisdictions and TRs in addressing the G20 reporting requirement implementation.

While a number of jurisdictions provide specific layouts of the fields and files, some do it for all OTC derivatives asset classes while others have different treatment for different asset classes or products. On the other extreme, a number of jurisdictions have not implemented data standards for TR data at all. In some cases, jurisdictions have chosen this approach intentionally by relying on relevant internationally accepted communication procedures and standards, while in other cases standardisation and harmonisation work is being undertaken but is not yet complete. In this context, some jurisdictions suggest the use of an UPI approach as a uniform product data standard for OTC derivatives data reporting in their rules and also the use of a UTI as a transaction identifier. However, there are currently no internationally accepted UPI and UTI standards. Among jurisdictions that have prescribed standards for products, they mostly cover credit, currency, equity and interest rate OTC derivatives although the coverage varies from jurisdiction to jurisdiction. Very few jurisdictions have developed data standards for commodity derivatives, particularly the identification of the underlier.

While some authorities do standards development and maintenance on the regulatory level, others outsource that either to TRs or industry associations or similar bodies. Some authorities use a hybrid model of the above approaches.

A number of authorities indicated that they use some proprietary data items such as Reference Entity Database (RED) Codes[8] in their reporting requirements. However, it was noted that the proprietary licensed data standards seem to be used only for reporting of credit derivatives.

The application of tagging standards[9] also varies significantly among jurisdictions. In general, only a minority of authorities decided to implement data tagging standards for OTC derivatives reporting.

## 2.4 Legal and privacy issues

As previously pointed out in the FSB progress reports on the implementation of OTC derivatives market reforms, some jurisdictions have privacy laws, blocking laws and other laws that might prevent firms from reporting counterparty information and foreign authorities from reaching the necessary data from TRs. Some of the jurisdictions will address the issues

---

[8] Unique alphanumeric codes assigned to all reference entities and reference obligations, which are used to confirm trades on trade matching and clearing platforms.

[9] Tagging standards aim to increase the transparency and accessibility of business information by using a uniform format.

by changing/enacting new legislations, while others continue to work through possible solutions.

In most jurisdictions, TRs are permitted to disclose confidential information only to entities that are specified in law or regulation, and generally these entities include only authorities. In such cases, access to TR data may be provided to foreign authorities only if certain conditions are met, including, for example, the conclusion of an international agreement or MoU. In several jurisdictions, a TR may directly transmit data only to domestic (national or local) authorities. In some of these jurisdictions, foreign authorities may be granted indirect access to the data via national or local authorities, provided certain conditions are met, including, for example, MoUs between national/local and foreign authorities.

# 3. Authorities' Requirements for Aggregated OTC Derivatives Data

## 3.1 Data Needs

Both the Data Report and the Access Report broadly outline the potential data needs of authorities and provide guidance for minimum data reporting and access to TRs. The Data Report also discusses the importance of counterparty identifiers, a product classification system and trade identifiers, and makes general recommendations on how to achieve adequate aggregation. The Access Report focuses on the access requirements of authorities under different mandates and the procedures that facilitate authorities' access to TR data.

In order to categorise the diverse needs of authorities for aggregated data across TRs, this feasibility study follows the functional approach employed in the Access Report. This approach maps data needs to individual mandates of an authority and their particular objective rather than to a type of authority. These mandates may evolve over time. They include (but are not limited to):

- Assessing systemic risk,
- Performing general macro assessments,
- Conducting market surveillance and enforcement,
- Supervising market participants,
- Regulating, supervising or overseeing trading venues and financial market infrastructures (FMIs),
- Planning and conducting resolution activities,
- Implementing currency and monetary policy, and lender of last resort,
- Conducting research to support the above functions.

Appendix 3 describes these mandates as defined in the Access Report.

The mandates differ considerably in their requirements for data aggregation. For example, authorities conducting market surveillance and enforcement in most cases only need data from market participants and infrastructures in their legal jurisdiction (although they may also need data from market participants of other jurisdictions in cases where a contract is based on an underlying asset from their jurisdiction or if they jointly oversee market infrastructures,

e.g. CCPs, in foreign jurisdictions). They are frequently also supervisors of the TRs where their market participants report, potentially giving them greater access and control of data. In contrast, other mandates require access to a certain depth and breadth of data across a wider set of participants and underliers, which would not lend itself to a narrow jurisdictional view. For instance, authorities who assess systemic risk or perform general macro assessments have the need, according to the Access Report, not only for data on counterparties within their jurisdiction but also for anonymised data on counterparties outside their jurisdiction. These data are needed to assess global vulnerabilities and spill-overs between markets. Obtaining these data in a usable format requires the collection of data from many TRs in a consistent format, with consistent interpretation, with duplicates removed and identifying information masked, as described below. It also requires the creation of aggregate-level data on exposures.[10] Prudential supervisors similarly need data going beyond their market in order to assess the exposures of firms at a globally consolidated level.[11] For these mandates, a global aggregation solution is essential for providing adequate transparency to the official sector concerning the OTC derivatives market. Currently, no authority has a complete overview of the risks in OTC derivatives markets or is able to examine the global network of OTC derivatives transactions or positions in depth.

The complex set of needs of various authorities calls for an aggregation mechanism providing flexibility and fitted for evolutionary requests as financial markets and products evolve. It is also equally important for such a mechanism to be able to respond to evolving needs for aggregated data by authorities.

To provide authorities with the aggregated data consistent with the Access Report, various types of data aggregation will be necessary to complement the data that authorities may directly access from TRs. Some of the most important processes that are essential for aggregating TR data are described in the following sections.

## 3.2 Aggregation Minimum Prerequisites

The following requirements are core to any aggregation of OTC derivatives data for all types of mandates. These requirements would apply regardless of the aggregation model used. Box 1 illustrates the various aggregation needs through some sample uses of TR data by authorities with particular mandates.

### *a) User Requirements for Data Standardisation and Harmonisation*

TR data originate from a wide range of market participants submitting data in a variety of formats over a variety of communication channels. TRs themselves have different interpretations of terminologies, reporting specifications and data formats depending on the rules in their jurisdictions and their own choices. Consistent standards on how data are submitted to TRs and on how TRs transmit data to the aggregation mechanism would greatly facilitate aggregation. For example, greater standardisation of reporting requirements between jurisdictions and the completion of the implementation of key global standards such as LEIs,

---

[10] See Section 3.3(b) for further discussion of user requirements for calculation of exposures.

[11] For instance, prudential supervisors need aggregated data to assess the soundness of entities operating in multiple jurisdictions, such as data on credit risk (counterparty exposures), market risk (data on net position, valuation and collateral), overall liquidity risk (data on periodic contractual cash flows in OTC derivatives)

UTIs and UPIs are needed. Where data standards and interpretations are different, TR data must be transformed into a common and consistent form for use in analysis on an aggregated level. This can be difficult and perhaps in some cases impossible.

Some important examples of necessary areas for harmonisation are:

- the meaning of terminologies (e.g., transaction, position, UPI, whether the quantity of a transaction or of a position is expressed in the number of contracts or their value, etc.),
- the standard and format for expressing the terms of a transaction (such as the transaction price, quantity, relevant dates, and terms specific to certain types of securities such as rates, coupons, haircuts, value of the underlying, etc.) and whether a transaction is a price-forming trade,
- the identification of trades that are submitted for clearing and the child-trades created as a result. In some jurisdictions transactions once cleared must be reported as being modified transactions, while in other jurisdictions, the clearing results in the required reporting of both the termination of the initial transaction and the initiation of the new ones ("alpha-beta-trade" issue).

### *b) User Requirements for Concatenation*

Data necessary for fulfilling authorities' mandates may be held in several individual TRs in different locations. This is the result of competitive forces as well as regulatory requirements in various jurisdictions. Data are, therefore, physically and logically fragmented. The current landscape is described above in Chapter 2.

In order to obtain the needed data, each authority needs legal access and, absent a central aggregation mechanism, technical connections to each TR containing relevant data. Certain analyses can be accomplished with a narrower scope of data. For example, the mandates "Registering and regulating market participants" and "Supervising market participants with respect to business conduct and compliance with regulatory requirements" can be accomplished with data only from the (potentially small) number of TRs where specific market participants report. In contrast, the mandate "Assessing systemic risk" requires data from essentially all TRs and therefore needs a great deal of concatenation. An aggregation mechanism would help address a challenge which exists currently where an authority may not know which TR holds data relevant to its mandate, given the proliferation of TRs and the various reporting requirements in different jurisdictions.

### *c) User Requirements for Removal of Duplicates*

An important issue inherent in OTC derivatives data is the problem of duplicate transaction records, or "double counting". Duplicate records could potentially be collected and stored in several TRs within and across jurisdictions. Most data uses require that duplicate records be removed during the aggregation process in order to obtain accurate aggregated results. This is a key consideration for any data aggregation model, as duplicate event records can only be removed prior to manipulation of data such as summing or position netting, and identification of duplicate records is difficult unless the data contains key identifiers such as transaction identifiers or counterparty identifiers. For technical aspects of de-duplication please see Section 5.2.2.

### *d) User Requirements for Anonymisation*

Under certain mandates, authorities only have rights to obtain anonymised data and may be legally prevented from obtaining named data. Other mandates additionally require access to named data, at least for participants and/or underliers located in an authority's jurisdiction. Records can be **fully anonymised**, where the counterparty name or public identifier such as LEI is redacted and counterparty identity cannot be inferred from the remaining information. Alternatively, records can be **partially anonymised**, or masked, where counterparties are given unique identifiers that are used consistently across the entire dataset. Once raw transaction event data are fully anonymised, the derivation of position data or other summing by counterparty is not possible and removing duplicates would be very difficult. Summing of data by counterparty is needed for many types of network and systemic analysis as well as for netting data on gross bilateral positions. Partial anonymisation allows a user to construct positions or otherwise sum up raw events by counterparty, without knowing the actual identity of that counterparty, and also allows for the removal of certain duplicate records. However, in some cases it may also in practice allow identification of the counterparty from the raw information. Hence, the system of partial anonymisation should ensure that data cannot be reverse engineered to identify and expose those data elements that have been anonymised. For technical aspects of anonymisation and masking please see Section 5.2.1.

An alternative method for distributing at least some of the data that authorities need in a manner that protects the confidentiality of named counterparties and trade details is for a global aggregation mechanism to distribute to authorities aggregate-level data such as reports of global trade activity where information about individual counterparties cannot be deduced from the data.

### *e) User Requirements for Obtaining Timely Data*

Authorities have a need for both regular requests and ad hoc requests. Routine requests would typically come at monthly or quarterly intervals (or other pre-defined regular intervals). In some cases, in particular during periods of market stress, rapid responses to ad hoc requests will be important (e.g. provision of data within a few days).

## 3.3 Further aggregation requirements

Beyond the core aggregation steps discussed above, several other aggregation steps will be required under certain mandates. These steps should be considered as more optional for the initial design and implementation stage of the aggregation mechanism, since they could either be performed separately from the main aggregation mechanism and require significant legal change to operationalise.

### *a) User Requirements for Calculation of Positions*

Several mandates require information on the positions of market participants: the sum of the open transactions for a particular product and participant at a particular point in time. This will require tools to identify the transactions to be summed and de-duplicated. In particular:

- Counterparty identifiers (LEI) are required to accumulate accurate position data across TRs. The LEI with hierarchy (for consolidation purpose) is also needed for some mandates at least in a second step when the fully fledged LEI is in place.

- Product identifiers (ideally UPIs, and any other instrument identifier available) are needed to do accurate product-level analysis. Different analyses require different levels of product identification granularity.
- IDs of underliers (e.g. reference entity identifier, reference obligation and restructuring information in case of credit derivatives, reference entity identifier for equity derivatives, benchmark rate in the case of interest rate swaps and cross currency swaps) are required to conduct various analyses (for instance, to measure total exposure in a given reference entity, or to value the trades for any analyses where market values, rather than notional amounts, are aggregated and where the TR does not collect those market values).

### *b) User Requirements for Calculation of Exposures*

The current exposure of a derivative portfolio – defined as the cost of replacing the portfolio in current market conditions net of any collateral backing it – is an important measure of risk that is of interest to authorities. Calculating exposures requires not only position data, but also data on valuations, collateral (e.g., amount and composition of applied collateral) and netting sets. Such information includes external bilateral portfolios between pairs of market participants and portfolios of centrally cleared transactions (particularly important for including collateral information). IDs for collateral pools and netting sets will be necessary to connect multiple trades to their common collateral pool and netting sets. However, this data is not yet available in all TRs due to differences in regulatory requirements and, moreover, these types of unique identifiers are currently not yet fully operational.[12] Any aggregation solution should, however, take into account the requirements to calculate exposures where possible and to incorporate more complete data in the future. There is also a need for authorities to be able to calculate exposures combining aggregated OTC derivatives data with data on other related instruments. Due to the lack of these data in TRs, authorities will have to retrieve them from other data sources and aggregate them with relevant TR data in order to calculate comprehensive exposures.

[12] For instance, EU requirements include an ID for a collateral portfolio, although not collateral reporting per trade.

**Box 1:**
**Illustrations of data aggregation requirements**

This box illustrates the various aggregation requirements described above through some example of data uses of by authorities with particular mandates. Other uses by authorities with different mandates frequently encounter several of these issues.

**Business conduct supervision.** The first example relates to an authority with a mandate for supervising participants with respect to business conduct (see Annex 4 for data such an authority may have access to). This regulator suspects that a bank in its jurisdiction has traded on private information obtained during a loan renegotiation with a debtor by buying credit default swaps (CDS) that offer protection against potential losses due to the default of that debtor. Hence, the regulator wants to know the net amount of credit protection on the debtor bought by the bank over the past few days.

An aggregation mechanism would allow the authority to have a broader picture in order to detect violations. As the relevant CDS transaction event records may reside in a number of different TRs, they must first be brought together. Essentially these transaction records must be extracted from their respective TRs and concatenated. This could be done easily if each TR used the same data fields (with the same meaning/interpretation) and formats. Two particularly important data fields in this application are those containing the identities of the bank counterparty and the debtor referenced in the CDS contracts. These could be accurately searched if all TRs used the universal set of unique LEIs.[13]

As transaction events may have been reported to more than one TR, the regulator would want any duplicate records to be eliminated. If all TRs applied a UTI for each of the trades that they store, this could be done simply by eliminating any records from across TRs with duplicate UTIs.

Armed with a comprehensive and comparable list of duplicate-free transaction event records, the regulator could finally compute the net credit protection bought by the bank on its debtor over the past few days. It should do this by summing purchases of credit protection and subtracting any sales of credit protection. Only 'price-forming' trades should be included in this calculation.[14]

**Calculating positions.** A second example of data uses illustrates the aggregation requirement of calculating positions. It concerns a central bank with a financial stability mandate with a need to check whether any systemically-important firms in its jurisdiction have large OTC derivatives positions. Suppose that such an authority wanted to know the size of CDS positions referencing a particular country's sovereign debt sold by Bank A (including all its subsidiaries), located in its jurisdiction.

The transaction records that comprise this position potentially reside in a number of different TRs, so the authority would need the relevant trade records to be extracted and concatenated as in the first example. In this case, relevant contracts are any that end up with Bank A as the protection seller. This includes all contracts originally sold by Bank A but

[13] In addition, if the regulator asked authorities in other jurisdictions to search for any trades conducted by legal affiliates of the bank, it would be a simple matter to find their LEIs, given the LEI of the bank, once corporate hierarchy information is in place within the LEI system.

[14] Non-price-forming trades, such as those arising from compression cycles and central clearing, would not affect the bank's positions against the potential default of the debtor. They only affect the counterparties to these positions.

which have not yet matured or otherwise terminated. It also includes any contracts that were reassigned from the original seller of protection to Bank A. In both of these cases, the latest information about the trade contract would be needed, so any partial terminations or notional amount increases would also have to be extracted from the TR. After harmonising data standards and removing any duplicate transaction records, again as in the first example, the position of Bank A referencing that country's sovereign debt could finally be computed as the sum of outstanding transaction event records.

Expanding this second example brings in the aggregation requirement of anonymisation. Say the authority learned that Bank A had sold a large volume of credit protection on the sovereign debt of the country mentioned above. It might then want to know the overall degree to which market participants relied on Bank A for the supply of this insurance. Simple measures of market share require a comparison of the volume of protection sold by the bank with the overall level of protection sold by all market participants. More advanced statistical measures of network centrality take into account not only that many counterparties might rely directly on Bank A for credit protection, but that others might rely indirectly on Bank A having bought protection from a counterparty that in turn bought protection from Bank A. Computation of such measures requires data on all such links between counterparties as summarised in a matrix of bilateral positions, but the names of the protection buyers and sellers (other than Bank A) are not important. Hence, the names of these market participants could be partially anonymised before centrality is calculated.

**Calculating current exposures.** Finally, further expanding this example illustrates the aggregation requirement of calculating exposures. Say the authority was concerned about the solvency of a financial institution in its jurisdiction and, given the centrality of Bank A as a seller of an important type of credit protection, wanted to know if Bank A was exposed to this institution through OTC derivatives. Computation of this exposure first requires data on all outstanding positions across various OTC derivative asset classes between Bank A and the institution of concern (i.e. named data is required) and about which of these exposures are subject to netting arrangements. As in the first example, the positions can be calculated, after data harmonisation and removing duplicates, by summing all open transactions between Bank A and the other entity. Then it requires these positions to be valued. Some TRs may collect this valuation information, but others may not. Where it is not collected, derivatives positions may be valued using the prices of their underlying assets, which in some cases may be taken from a third-party database. This could be facilitated by the use both by TRs and third-party price providers of standard codes to identify underlying assets. In principle, any collateral posted against the market value of a bilateral derivatives portfolio after accounting for gains and losses within legal netting sets should then be deducted from that market value to determine the current exposure. However, not all TRs will collect this information and third-party sources of collateral data are much less readily available than for price data.

# 4. Legal Considerations

TRs are mostly regulated at the national level by national laws, and TRs that operate on a cross-border basis may be subject to more than one regulatory regime.[15]

Rules applicable to TRs usually concern the fields and formats for the information being reported (mandatory reporting), information being accessed (regulatory access) and organisational requirements. TRs are also usually subject to professional secrecy requirements, including relevant confidentiality/privacy/data protection laws.

The feasibility of Options 1, 2 and 3 in the current legal environment depends on the compatibility of the steps needed to implement these different options with the existing rules applicable to TRs. Legal challenges in implementing the different options stem from different levels of applicable law within a jurisdiction (e.g. sectoral legislation and/or confidentiality law of general application) as well as from cross-border issues.

It was noted in Chapter 3 that the establishment of common identifying codes (e.g., LEI, UPI and UTI) would greatly facilitate the aggregation process. In this context, changes to existing laws and regulations would be required to mandate the use, at local level, of global codes and formats (once they have been developed and internationally agreed).

This chapter analyses the legal considerations associated with the feasibility of the aggregation options described in Chapter 1 following three main dimensions: (i) the submission of the data to the global aggregation mechanism, (ii) access to data from the global aggregation mechanism, and (iii) the governance of the global aggregation mechanism. For each component, the chapter presents legal considerations associated with the implementation of each option.

The analysis focuses on the jurisdictions where TRs are established/registered/licensed[16], or will be in the short term, and pertains to the legal considerations applicable to data reported to TRs on a mandatory basis.[17]

The analysis assumes that the only counterparty information that would be included in the aggregation mechanism would relate to counterparties that are legal entities and not to counterparties that are natural persons. In the exceptional cases where TRs would hold data that enable the identification of natural persons[18] ("personal data"), this study assumes that

---

[15] The TR may be regulated in a jurisdiction other than its home jurisdiction, due to being registered, licensed or otherwise recognised or authorised in that jurisdiction, or conditionally exempt from registration requirements in that jurisdiction.

[16] Appendix D of the FSB's seventh progress report on implementation of OTC derivatives reforms provides a list of TRs operating or expected to operate as of April 2014. The list of jurisdictions where TRs are established/regulated/licensed includes: Brazil, European Union, Hong Kong, India, Japan, Korea, Mexico, Russia, Saudi Arabia, Singapore and the United States.

[17] There are two kinds of data reporting: mandatory reporting and voluntary reporting. The former is required by legislation and/or regulation, while the latter occurs without such legal requirements. The ability to share data reported to TRs on a voluntary basis raises different legal issues which are outside the scope of this study. The scope of the mandatory reporting requirements varies across jurisdictions (for example, there are differences between reporting of exchange-traded derivatives and OTC derivatives across jurisdictions, as well as differences regarding the reporting of collateral information).

[18] Personal data could include, for example, data about a natural person that is a counterparty to a trade, or data about a natural person that arranged the trade on behalf of a counterparty or that is a beneficiary of the trade. Trade Repositories attending the workshop held in Basel in November 2013 noted that the data they hold are essentially business data, and that personal data would be held in TRs only in exceptional cases.

personal data would not be included in the aggregation mechanism.[19] Besides the reference material mentioned in Chapter 1, the analysis of this chapter has also been informed by the FSB progress reports on the implementation of OTC derivatives reforms[20] which include descriptions of confidentiality issues related to the reporting of OTC derivatives into TRs. The analysis also builds upon the discussion of the International Data Hub relating to global systemically important banks (G-SIBs) and the LEI global initiative.

## 4.1 Types of existing legal obstacles to submit/collect data from TRs into an aggregation mechanism

### *4.1.1 Legal requirements applying specifically to the TR seeking to transmit data to the aggregation mechanism and regulating the TR's capacity to share data*

In the existing regulatory environment, a TR seeking to transmit information to an aggregation mechanism – either to a physically centralised aggregation mechanism (Option 1) or a federated aggregation mechanism (Option 2) may face legal obstacles in its home jurisdiction, or in other jurisdictions in which the TR is regulated.

In most jurisdictions legal requirements applying to TRs include limitations on the types of entities with which the TR may share data. These legal requirements may prevent TRs from transmitting confidential information to an aggregation mechanism, depending on which entity operates the central aggregator, and which authorities have access to the aggregation mechanism. Confidential information may not be limited to information that identifies the counterparties to a particular transaction but may also include the size of or other information specific to the terms of the transaction or may even include all non-public information.

In most jurisdictions, TRs are not permitted to disclose any confidential information to any person or entity other than those expressly authorised by laws, regulations or rules. This could include for example, a TR being authorised to share data with specified foreign and domestic authorities or with public-sector entities only. In some cases the list of entities with access to TR data is defined by law or subordinate legislation and may include foreign authorities.[21] In several jurisdictions, TRs may transmit data only to domestic authority(ies), which would prevent the TR from submitting data directly to an aggregation mechanism or to a foreign authority.[22] In some other jurisdictions, the TRs' supervisors may be authorised to designate foreign entities entitled to access data held in the TRs.[23]

---

[19] A more detailed analysis of the practical methods for local TRs to identify personal data so that it can be excluded from aggregation is recommended. For example, analysis should be carried out to determine whether it would suffice for local TRs to make available to the aggregator only positions associated with an LEI, as currently individual persons are not able to obtain an LEI.

[20] Fifth progress report, April 2013, http://www.financialstabilityboard.org/publications/r_130415.pdf
Sixth progress report, September 2013, http://www.financialstabilityboard.org/publications/r_130902b.pdf
Seventh progress report, April 2014, http://www.financialstabilityboard.org/publications/r_140408.htm

[21] Australia, European Union, Singapore and South Africa.

[22] Brazil, China, India, Korea, Mexico, Russia, Saudi Arabia and Turkey.

[23] United States.

In this context, the implementation of Option 1 and Option 2 (as this involves temporary local caching where necessary in the aggregation process) would require explicitly prescribing the aggregation mechanism (by amending existing laws or regulations where necessary in all relevant jurisdictions) among the entities entitled to access TR data.

Under Options 1 and 2, if the transmission of data from the individual TRs to the aggregation mechanism is performed on a routine basis, the TR may not know at the point of transmission which authorities will seek to access the data or for what purposes, and the TR therefore could not directly apply any access controls at its end. Where TRs are legally required to control access, they would be reliant on the aggregation mechanism to do so on their behalf. This outsourcing of controls might not be allowed in some jurisdictions without a change in law or regulation. If so, the issue would have to be addressed by the governance framework establishing the aggregation mechanism and regulating its access. The governance issue including access rules is further discussed in Section 4.3.

### *4.1.2 Legal requirements of general application*

*Privacy laws, blocking statutes and other laws that limit or prohibit reporting to TRs or regulatory access to data held in TRs*

A TR may also be subject to legal requirements of general application such as privacy laws, data protection laws, blocking/secrecy laws and confidentiality requirements in the relevant jurisdiction, which are applicable to all the options. These legal requirements may prevent the TR from transmitting certain types of information to an aggregation mechanism under Options 1 and 2 absent a change in law or regulation.

The legal requirements of general application that may prevent a TR from transmitting data to the aggregation mechanism under Options 1 and 2 may in some cases mirror obstacles that prevent participants from submitting data to a TR in the first instance. Those obstacles are more fully discussed in the FSB's fifth, sixth and seventh progress reports on OTC derivatives market reform implementation[24]. For example:

- privacy laws may prevent or restrict a TR from transmitting counterparty information to the central database (wherever located) where that information identifies a natural person or entity (in some instances, this restriction applies unless certain conditions are met such as the provision of consent);
- blocking laws may prevent or restrict a TR from transmitting/disclosing information relating to entities within a particular jurisdiction, to third parties outside that jurisdiction and/or to foreign governments.

In some jurisdictions, the TR may be able to rely on exceptions to privacy laws expressly listed in the laws or where there is a counterparty's express written consent to the disclosure of the data. However, the requirements for consent differ across jurisdictions. In certain jurisdictions, one-time counterparty consent to disclosure to a TR is sufficient, while in others counterparty consent may be required on a per-transaction basis. In any case, relying on

[24] See section 3.2.1. http://www.financialstabilityboard.org/publications/r_130415.pdf, section 6.3.1 of http://www.financialstabilityboard.org/publications/r_130902b.pdf and section 2.1.2 of http://www.financialstabilityboard.org/publications/r_140408.pdf.

counterparty consent is not an effective long-term solution, and changes to law or regulation will still be required to enable an effective implementation of Options 1 or 2.

*Consequences of breach*

As noted, the source of the above legal requirements may be laws, regulations or rules of the jurisdiction in which the TR is located, of another jurisdiction in which the TR is regulated, or of a jurisdiction in which the counterparties to a transaction are located. Other sources of these requirements may be conditions of the TR's registration, licensing or other authorisation in a particular jurisdiction, or contractual arrangements to which the TR is a party, including the TR's own rules and procedures. These conditions or contractual arrangements may be designed to support compliance with local laws, e.g., privacy laws.

A TR that breaches these legal requirements may be exposed to civil liability or criminal sanctions in the relevant jurisdiction. Further, if a TR is required to ensure that the entity that operates the aggregation mechanism, or authorities that have access to the aggregation mechanism comply with specified requirements (e.g., undertakings as to confidentiality) with respect to the data transmitted, the TR may be exposed to liability if the aggregation mechanism or authority breaches those requirements. Authorities who might even unwittingly contribute to such a breach, or fail to prevent one, could be subject to litigation and legal challenges.

These potential obstacles, unless addressed, could limit the capacity of the TR to transmit confidential data to the aggregation mechanism, and could therefore limit the range of data held in the aggregation mechanism, which might prevent authorities from accessing all the information they need in carrying out their regulatory mandates.

### *4.1.3 Factors mitigating the legal obstacles to transmission of data by TRs*

*Type of data being transferred: anonymised and aggregate-level data*

The legal obstacles may differ depending on the type of data being transferred to the aggregation mechanism under Options 1 and 2. TRs sending aggregate-level data or data in anonymised[25] form to the central aggregator could mitigate most of the confidentiality issues identified above which apply to the transmission of confidential data.

On the other hand, it should be noted that transmission of data that has already been anonymised (e.g., with no LEI or other party-related information) or that has already been summed faces serious drawbacks, such as the inability to eliminate double-counting and the inability to perform calculations of positions or exposures as discussed in Chapters 3 and 5.

*Authorities acting as intermediaries for the transmission of data into the aggregation mechanism and legal status of the aggregation mechanism*

The legal status both of the provider of data and of the aggregation mechanism can affect the ability to provide data to the aggregation mechanism. In cases involving TRs organised as

[25] A methodology to do so would need to be further defined and demonstrated. Different types of anonymisation are described in Chapter 3. The methodology would need to address the issue that, in some circumstances, anonymised counterparty identities may be ascertainable e.g. based on historical trading patterns or account profiles, or because of lack of depth in the market.

private entities rather than authorities, the transmission of the data from TRs to the aggregation mechanism via authorities may alleviate some of the legal concerns identified above. Many authorities have, unlike TRs, the capacity to share confidential information with authorities and, in some instances, private sector entities, provided certain conditions are fulfilled, notably within existing frameworks of cooperation arrangements for data sharing.[26] However, the implementation of a mechanism where the information would flow via authorities would face some practical obstacles given the large volume of data involved.

The effectiveness of using an authority as an intermediary could also be affected by the legal status of the aggregation mechanism itself. More specifically, if the mechanism is structured as a public entity that meets the existing definitions of "authority" or as an entity with whom information can already be shared on a confidential basis (which could include international financial institutions in some instances), sharing of information could be facilitated both from the TR directly and via the relevant authority. However, depending on definitions across jurisdictions, legislative changes may still be needed to include or designate such a public entity in the framework for information sharing.

### 4.2 Legal challenges to access to TR data

In some jurisdictions, direct access by foreign authorities to data held in local TRs is permitted, while it is not in other jurisdictions. In most jurisdictions, foreign authorities may be granted indirect access to the data via national authorities on an authority-to-authority basis – usually from the supervisor of the TR (or after approval of the supervisor) – provided MoUs or other necessary processes have been concluded. In some jurisdictions, access on an authority-to-authority basis may be the only avenue.[27]

In most jurisdictions, direct access by regulators to TR data is provided for by law and can include access by foreign authorities, provided certain conditions are met. These conditions may include the conclusion of MoUs – or specific types of international agreements[28] – between relevant authorities on data sharing. As another example, a TR may be required to take specified steps before sharing information with an authority, such as ensuring that an agreement or undertaking as to confidentiality, or indemnification[29] in respect of potential litigation, is in place with the requesting entity.

---

[26] Indeed, while TRs are usually subject to laws and/or regulations that prevent them from sharing confidential information (e.g., with foreign authorities), TRs' regulators, or other entitled authorities, may be empowered to access and share confidential information held in the TRs they supervise with other foreign authorities under international cooperation arrangements (such as MoUs) related to the exchange of information between regulators or cooperation in supervisory activities. Direct access by foreign authorities to data held by TRs organised as private sector entities is typically subject to other data protection safeguards.

[27] Brazil, Russia and Turkey.

[28] For example, in the EU, as a condition for direct access to EU-regulated TR data by third country authorities from jurisdictions where TRs are established, the European Market Infrastructure Regulation (EMIR) requires that international agreements and co-operation arrangements that meet the requirements of EMIR be in place between the third country and the EU. For third country authorities from jurisdictions where no TR is established, EMIR requires the conclusion of cooperation arrangements.

[29] For example, in the US, the Dodd-Frank Act requires that, as a condition for obtaining data directly from a TR, domestic and foreign authorities agree in writing to indemnify a US-registered TR, and the SEC and CFTC, as applicable, for any expenses arising from litigation relating to the data provided. The CFTC issued a final interpretative statement, and the SEC proposed relief.

Under Options 1 and 2, authorities would access global OTC derivatives data via the aggregation mechanism. A new international framework specifying who may access the data, the coverage of the information that may be accessed, and the conditions for access would therefore need to be globally agreed, as noted in the governance section below. This framework for access would need to reflect any legal conditions under which the data was transmitted to the aggregation mechanism. It is assumed that such a framework to be set up to implement Options 1 or 2 would include within its design solutions to the existing access issues identified above.

If an agreement at global level is reached to implement Option 1 or 2[30], relevant authorities would access global data on OTC derivatives through the aggregation mechanism (see the table in Chapter 1). The governance framework for the aggregation mechanism, including any global-level agreements required to establish such a mechanism, could act as a substitute for the bilateral agreements that are currently required in many cases to access data at individual TRs. Under Options 1 and 2, if TRs are responsible for submitting the data they hold into the aggregation mechanism, the new international framework could also be designed, in combination with any necessary amendments to local laws and regulations, to ensure that TRs are able to transmit the data without legal impediments.[31]. Under Option 3, authorities would access information directly at TRs. Option 3, like Options 1 and 2, would depend on both the completion of additional steps required under the existing regulatory frameworks to permit access to TRs by authorities worldwide (such as the conclusion of bilateral international agreements or MoUs) and changes in the existing legislative and regulatory frameworks where access at TRs is not permitted or is limited by legal obstacles (e.g., indemnification provisions).

## 4.3 Legal considerations for the governance of the system

### *4.3.1 General analysis*

The objective of this section is to analyse the legal considerations related to the governance of the aggregation mechanism for each option proposed, analysing what would likely need to be defined and agreed internationally to ensure the global aggregation mechanism could be implemented and managed. As highlighted in Chapter 1, the objective of this study is not to define the specific governance requirements, but rather to highlight the various governance considerations that would need to be addressed for the implementation of each option. Additional work on the legal considerations and appropriate allocation of responsibilities surrounding governance and operational issues would need to be undertaken at a later stage as part of the planning work for a global aggregation mechanism, and before undertaking any more formal project development.

Options 1 and 2 require a global framework to be defined specifying: (i) which entity would operate the aggregation mechanism, (ii) how the aggregation mechanism would be managed and overseen/supervised, (iii) access rules (which authorities would have access to which information according to their mandate and confidentiality restrictions in the use of data),

[30] The Agreement could take the form of international agreements or a multilateral MoU.

[31] Other legal issues, e.g. indemnification issues, would still need to be solved.

(iv) the entity accountable for any breach or failures in the system, and (v) mechanisms for resolving disputes around access rights.

Under Option 1, a physically centralised aggregation mechanism would be established to collect and store data from TRs. This aggregation mechanism would subsequently aggregate the information and provide it to relevant authorities as needed. Some changes to the existing legislative and regulatory frameworks would be required to set up an aggregation mechanism entitled to collect confidential information stored in TRs. The framework for Option 1 would further require specifying the location of the physically centralised aggregation mechanism and the information to be collected and stored there (including maximum storage/retention period for the data).

Option 2 would not physically collect or store data from TRs in advance of a data request, instead it would rely on a central logical catalogue/index to identify the location of data resident in the TRs. In this model, the underlying data would remain in TR databases and be aggregated via logical centralisation by the aggregation mechanism, being retrieved on an "as needed" basis at the time the aggregation program is run. The framework for Option 2 would further require agreeing on: which information would be incorporated into the central logical catalogue/index for logical centralisation and access; and the responsibilities of the aggregation mechanism and how the federated aggregation mechanism would be operated (e.g. whether it is in charge of performing de-duplication, anonymisation, etc. as discussed in Chapter 5).

Under either Option 1 or 2, further analysis would also be needed to better determine how such a mechanism should be structured, including, for example, whether it would be a private or public entity.

Option 3 would not require setting a global governance system, as it is largely dependent on negotiating authority-to-authority agreements that would set forth access rights and responsibilities. However, it would require the conclusion of international agreements (cooperation arrangements, memorandum of understanding, etc.) between relevant authorities and resolution of indemnification issues, as mentioned in the previous sections, to fully enable relevant authorities to access global data on OTC derivatives.

### *4.3.2 The need for global governance frameworks under Options 1 and 2*

Assuming an international commitment to set up an aggregation mechanism for OTC derivatives data, different possible governance approaches would permit the implementation of such a mechanism.

*Considerations for defining the entity running the database and the global supervisory/oversight framework*

Under Options 1 and 2, the global framework would likely need to define which entity operates the aggregation mechanism and in particular the nature of the entity that may run and manage the aggregation mechanism and how this entity could be supervised/overseen (if a private entity) or otherwise governed (if a purely public entity). At least two cases can be envisaged, depending on whether the database is run via a public-private partnership (cf. model of the LEI initiative) or if the central database is operated by a public entity (cf. model of the Data Hub).

- *Public-private partnership*

In the current landscape of TR services providers, several global companies operate TRs established in various jurisdictions, offering TRs services in line with each jurisdiction's local requirements. The existence of companies running TRs in different jurisdictions could pave the way to building a global infrastructure that would aggregate the information contained in individual TRs on a not-for-profit basis and subject to public sector governance. In that regard, the LEI initiative provides an insightful example comprising a public-private initiative, leveraging the knowledge and experience of local infrastructures, with a global regulatory governance protecting public interest and open to all authorities worldwide.

Several models could already be envisaged for the supervision/oversight of an aggregation mechanism on OTC derivatives data operated by a private entity. The private entity running the aggregation mechanism could be supervised or overseen by a college of authorities from different jurisdictions, which would set up a global supervision/oversight framework. Another framework would rely on the direct supervision/oversight of the private entity by an international institution under a global governance framework.

The global governance framework of the LEI initiative is an example of a global governance framework which was set up in a relatively short time frame (set up in two years from the G20 mandate to the first operationalisation). However, aggregation of TR data is a far more complex task than the generation of an LEI code, in particular given the volume and complexity of the data handled. The key elements from the LEI initiative, which could be helpful in designing a global framework governing a TR data aggregation mechanism if run by a private entity, are summarised in Box 2.

**Box 2:**
**Global LEI initiative**

**G20 mandate** to FSB (Cannes Summit, November 2011)

The LEI initiative includes a four-tiered system with a governing charter for the Regulatory Oversight Committee (ROC)[32], a Global LEI Foundation operating the Central Operating Unit as well as the federated local operating units.[33] The initiative makes use of the LEI identification standard provided by the International Organisation for Standardisation (ISO) – ISO 17442 – designed to ensure the unambiguous identification of the counterparties engaging in financial transactions. In this framework the ROC will take ultimate responsibility for ensuring the oversight of the Global LEI system, standards and policies.

**– the ROC,** established by Charter set out by the G20 and FSB. Members are authorities from across the world. Responsibility for governance and oversight of the Global LEI system, and delivery of the broad public interest.

The following are eligible to be a Member of the ROC: (1) any public sector authority and jurisdiction including regulatory and supervisory authorities and central banks; (2) public international financial institutions; and (3) international public sector standard setting, regulatory, supervisory, and central bank bodies and supranational authorities.

[32] http://www.leiroc.org/publications/gls/roc_20121105.pdf

[33] See FSB report – http://www.financialstabilityboard.org/publications/r_120608.pdf

**– Global LEI Foundation**, governed by independent Board of Directors (composed with balance between technical skills, sectoral experience, geographic balance). Upholds centrally agreed standards under a federated operating model. Will be established as a not-for-profit foundation in Switzerland. Will operate central operating unit. FSB acts as a Founder of the foundation.

**– Local Operating Units**. Build on local knowledge, expertise, and existing infrastructures. Operate to centrally agreed standards under the federated operating model.

The FSB report, "A Global Legal Entity Identifier for Financial Markets", highlights the creation, governance and function of a global LEI system.

- *Public entity*

An aggregation mechanism could also be run by a public entity. Given the nature of the data that is collected based on mandatory reporting requirements, establishment of public entity might be less complicated from a legal perspective. Several authorities note being authorised to provide information to foreign authorities, bodies or to entities carrying out legally mandated obligations. Although there will still be significant challenges in creating a mechanism, having the mechanism organised as or run by a public entity could more easily facilitate provision of data.

The Data Hub on global systemically important banks (described in Box 3 below) has been recently established by the BIS through the conclusion of a Multilateral Memorandum of Understanding.

The legal framework applicable to the Data Hub is a useful starting point for considering the implementation of Options 1 and 2, in the sense that the hub centrally collects global financial data, including confidential data, and is able to share this information with relevant authorities. A similar governance framework could be envisaged for an aggregation mechanism comprising a public entity operating the infrastructure and the establishment of an international Governance Group. While the Data Hub is designed to be a connector among regulators, the aggregation mechanism being discussed in this report could be directly connected to TRs, albeit under regulatory oversight.

**Box 3:**
**The International Data Hub**

As part of wider G20 initiatives to improve data to support financial stability, the FSB has developed an international framework that supports improved collection and sharing of information on linkages between global systemically important financial institutions and their exposures to sectors and national markets[34]. The objective is to provide authorities with a clearer view of global financial networks and assist them in their supervisory and macro-prudential responsibilities.

The key components of the governance of this initiative are the following:

[34] See recommendations 8 and 9 of the Report to the G20 Finance Ministers and Governors on "The Financial Crisis and Information Gaps" from November 2009, available at http://www.financialstabilityboard.org/publications/r_091029.pdf.

**– Harmonised collection of data**: common data templates for global systemically important banks have been developed under the FSB leadership to ensure consistency in the information collected.

**– Central hub**: The International Data Hub has been set up[35] and centrally holds the data collected. The data hub is **hosted by the Bank for International Settlements** (BIS). A multilateral memorandum of understanding (Multilateral Framework) establishes the arrangements for the collection and sharing of information through the Hub. Currently, the Framework is signed by banking supervisory authorities and central banks from ten jurisdictions. Access of these jurisdictions to confidential information is contingent on the reciprocal provision and restricted to specific purposes such as supervisory activities.

**– GSIBs data is collected by their respective home authorities** (data providers) and then passed on to the Data Hub. Data providers use their best efforts to ensure the quality of the data transmitted to the Hub. The Data Hub prepares and distributes **standard reports** to participating authorities (data receivers) on a regular basis. In addition, data receivers can require additional information from the Hub, which fulfils the request after obtaining written consent from data providers.

**– Hub Governance Group**: Participating authorities established a Hub Governance Group (HGG) to oversee the pooling and sharing of information. The HGG is responsible for all governance aspects of the multilateral arrangement.

*Considerations for the submission of data to the aggregation mechanism and addressing confidentiality issues*

The global governance framework would likely need to define how the aggregation mechanism collects data from local TRs. Two cases could be envisaged at this stage.

Firstly, the aggregation mechanism framework could be built on a global agreement mandating local TRs to submit relevant data (to be agreed on, which might or might not include confidential information) to the aggregation mechanism – and, where needed, changes to regulatory frameworks enabling the implementation of mandatory reporting to an aggregation mechanism. Requiring by law for the local TRs to report to the aggregation mechanism with the conclusion of a Multilateral Memorandum of Understanding for cooperation among relevant authorities would address, in most jurisdictions, the confidentiality obstacles identified above. This would however require a change in law in most jurisdictions and, potentially in addition, rule-making or similar actions by relevant authorities.

Secondly, the aggregation mechanism framework could be built with information flowing via national authorities, as described under section 4.1.3. This is the approach followed for the Data Hub: national authorities transmit data (including confidential information) on G-SIBs to the central hub, which is entitled to centrally hold and share confidential information with relevant authorities participating in the framework.[36] As in the case of the Data Hub, the

[35] The Hub operations started in March 2013 with the collection of weekly data on the G-SIBs' 50 largest exposures and quarterly data on aggregated claims to sectors and countries.

[36] However, given the volume of data at stake for OTC derivatives, an automated process enabling national authorities to forward the relevant data to the database would be required.

protection of confidential data would have to be addressed via the conclusion of Multilateral Memorandum of Understanding.

Strict confidentiality rules applying to the aggregation mechanism may also need to be defined. Laws applicable and confidentiality requirements in the jurisdiction where the aggregation mechanism resides and where data are stored either permanently under Option 1 or temporarily under Option 2 will be key components of the framework.

### *4.3.3 Considerations on access rules*

Under Options 1 and 2, authorities would access global OTC derivatives data directly at the aggregation mechanism. The global governance framework would therefore need to define rules on access to the information held at the central aggregation mechanism. These rules may need to specify:

- Who may access the aggregation mechanism (list of relevant authorities, official international financial institutions[37], etc.).
- Scope of data access: the assumption in this report is that the aggregation mechanism would provide authorities with a level of access in line with the principles defined in the Access Report.
- Permitted use of data: the permitted uses for financial stability purposes and other relevant mandates would need to be defined, as would protection of confidential information that is accessed and consequences of any breach.
- Modalities of access (direct vs indirect access, standard vs ad hoc requests).

Under Option 3, individual authorities directly collect the raw data they need from individual TR databases and then aggregate the information themselves within their own systems. This option can be implemented in the existing legal frameworks, if each relevant individual authority has access to the information it needs in all relevant TR databases.

The implementation of this option would therefore require solving the existing legal obstacles relevant to access to data (described in the previous section) in order to ensure that the legal frameworks applicable to TRs in each jurisdiction allow access to TR data by relevant foreign authorities:

- granting access to foreign authorities in the few jurisdictions where foreign authorities are not entitled to access TR data,
- addressing the indemnification issues in jurisdictions where access to TR data by foreign authorities is conditional on the indemnity clause,
- concluding the necessary Memorandum of Understanding, and/or
- concluding other types of international agreements in jurisdictions that require them under law.

[37] In the Access Report, the IMF, the World Bank and the BIS are stated as official IFIs that foster and support financial stability through general macro assessments of global OTC derivatives markets, sectors or specific countries.

It should be noted that, under Option 3, unless there is a global agreement providing further detail and specificity as to what data each type of entity is entitled to receive (such as would be provided in the framework for an aggregation mechanism), TRs as gatekeeper may interpret conservatively the minimum requirements for access set in the Access Report. This could lead to arbitrary decisions regarding the evaluation of mandates as well as what kind of data should be shared for each mandate.

In that regard, and more broadly to streamline the legal arrangements needed to support the implementation of Option 3, one possibility would be to envisage the conclusion of a multilateral arrangement under which the participating authorities (or jurisdictions) would agree on reciprocal access to TR data.

# 5. Data & Technology Considerations

The development of technical and data solutions for collection and aggregation of data from TRs has been, to date, largely at the local level. Technical aggregation solutions are at the earliest stages of development in most jurisdictions. Data requirements differ both between jurisdictions and between TRs within jurisdictions. The necessary definitions, standards and formats are either absent or being developed at the level of individual jurisdictions or TRs. Under these conditions, provision by TRs of data for aggregation is difficult within jurisdictions and not possible on a global scale. In addition, data aggregation faces particular data challenges due to the need to remove duplicate transactions and, in some cases, anonymise data.

## 5.1 The Impact of the Aggregation Option on Data and Technology

Many of the data and technology requirements described in this chapter apply independently of the chosen aggregation option and therefore do not drive the choice of aggregation model. An important example is the development of global standards for derivatives data and their aggregation, which is a foundational requirement for the interoperability of derivatives data under any data aggregation model. The appropriate content of the standards is agnostic to the choice of aggregation option.

Options 1 and 2 share many data and technology requirements, with their needs differing only at the margin. Both options require a shared catalogue to identify where data resides and the implementation of a central technical infrastructure to collect, manipulate and distribute data. Data storage requirements are higher for Option 1, although Option 2 would also require temporary data storage for indexing, processing and caching purposes.

## 5.2 Data aggregation and reporting framework

In any data reporting or aggregation framework, data is accessed through a request (ad hoc or pre-defined) submitted to the system. The system performs the following functions:

- verifies the identity and access rights of the data requestor;
- analyses the request according to the data scheme, syntax and semantics;
- controls its consistency and integrity;

- optimises it for the purpose of execution;
- executes the request according to storage scheme and access methods;
- assesses completeness of results and provides the results to the requester;
- checks the performance of the aggregation mechanism and network performance (e.g. response times, latency, traffic bursts).

In the TR data aggregation context, the complexity of servicing a request for execution increases since the data might be stored in different physical locations, and be subject to different access rights, data standards and technology solutions, with possibly different access methods and storage schemes.

Two particular technical functions are important for any aggregator: anonymisation and de-duplication.

### *5.2.1 Anonymisation and masking*

As initially discussed in Section 3.2, certain counterparty data can only be given to authorities in an anonymised form. On a more technical level, data may be fully anonymised or partially anonymised in the following manner:

- Data is **fully anonymised** where the counterparty name or public identifier (such as LEI) is redacted. Full anonymisation also implies the removal of UTIs from the data because, as currently constructed, they are based on codes that identify participants or trading venues. This type of anonymisation is simple and can be performed on different datasets of raw transaction events prior to concatenation. For example, TR A and TR B can themselves remove counterparty names from their respective datasets before sending to a third party (central aggregator or user) to combine.
- Alternatively, records can be **partially anonymised, or masked**, where counterparties are given unique identifiers that are used consistently across the entire dataset. For example, the identifier "1234" could be assigned to Market Participant X and "5678" to Market Participant Y. Partial anonymisation could be performed by a single central party, i.e., the aggregation mechanism, to perform the masking on a given dataset. Partial anonymisation could also be performed locally in TRs, based on a set of agreed-upon and consistent anonymisation rules and translation data.

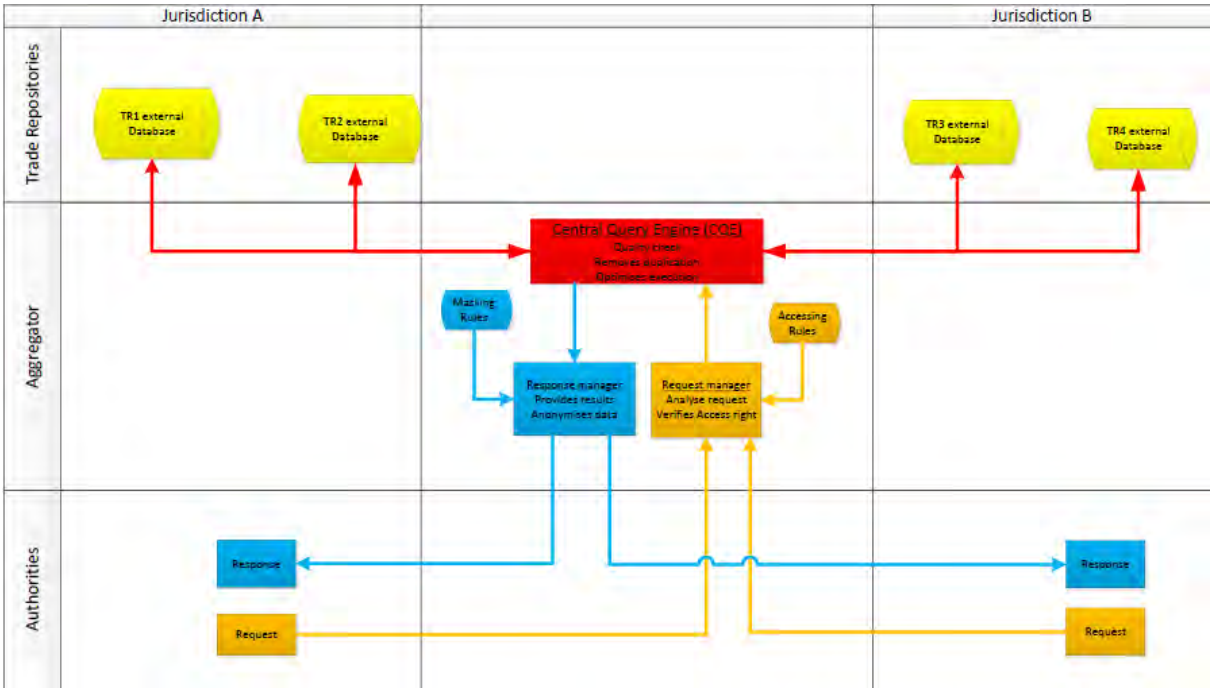
  The data masking can be static or dynamic. Static masking transforms the data, making them anonymous, and deposits them in another database. Dynamic data masking is a technology that avoids the need to change the applications or databases. Instead, sensitive information is masked by means of software (middleware) that allows the management of access levels for each piece of data at the time the software runs.

There are a number of practical approaches to implement partial anonymisation or masking. Two examples are proposed below, both based on Option 2, but that can also be implemented with Option 1. The feasibility of each approach will depend on how the legal and regulatory environment evolves. In the first example the aggregator would perform the anonymisation. In this case it would be possible to perform cross-jurisdiction aggregation and then present the data to users. The second example is more restrictive from the point of view of the

confidentiality of data, with masking performed at the TRs, but less useful for cross-jurisdiction aggregation.

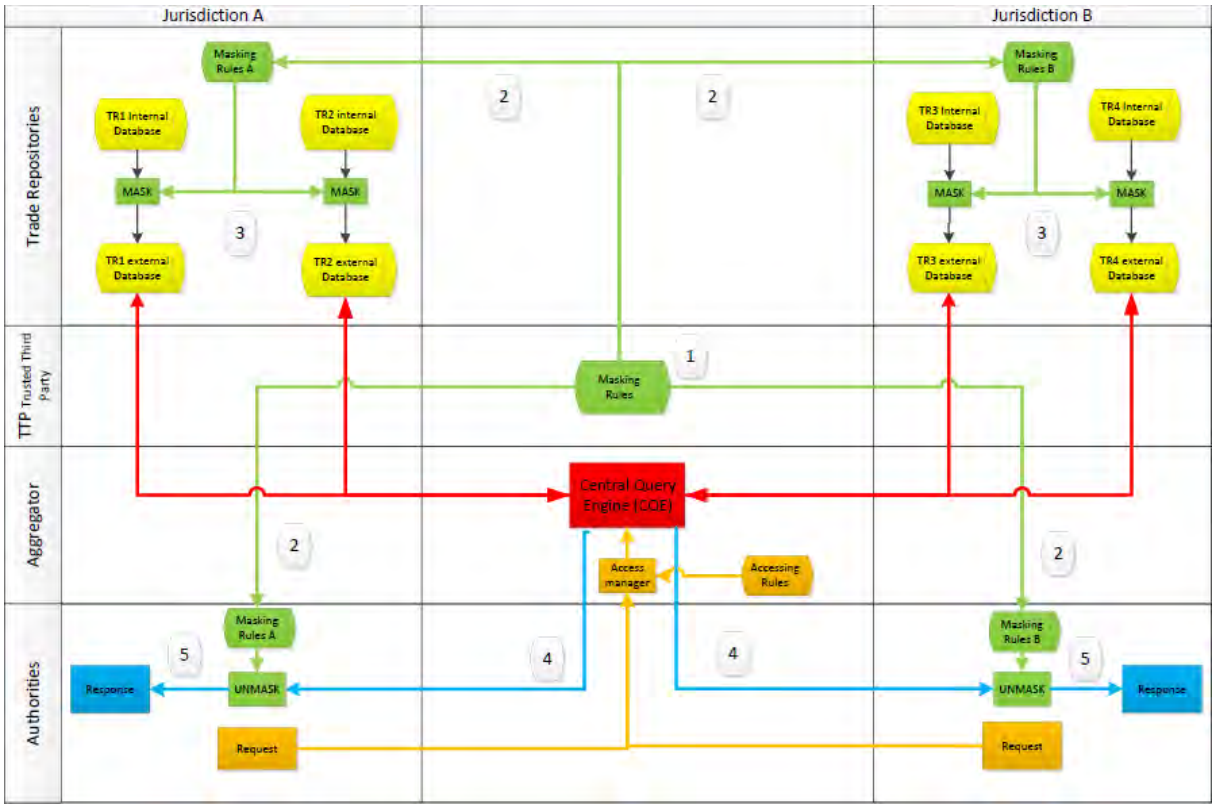
1) The central aggregator performs the anonymisation after concatenating data from TRs, taking account of the access rights of the authority requesting the data. This approach might be more acceptable if the management of the aggregator was entrusted to a public entity with strong governance and security policies.

***[Illustration of a possible approach of the above example where the masking is done dynamically for different uses and users]***




2) 2) This solution uses a key that maps true LEIs to masked LEIs. The masked LEIs look like random alpha-numeric codes. The key would be created by, for example, a trusted third party (TTP). The TTP would be independent of the central aggregator and would never share the key with it. Instead, the key would be shared with the relevant trade repositories and authorities. Trade repositories would use the key to mask LEIs before sending the data to the central aggregator. The central aggregator would deliver the data with masked LEIs to authorities. This data could be raw or derived (calculated). The TTP would need a list telling it which keys could be sent to which authorities. On receipt of this information, authorities would use the key to unmask only the LEIs of the institutions to which their query results related.

***[Illustration of a possible approach of the above example where the central aggregator does not have access to named data]***




It should be emphasised that these two examples are included to demonstrate the scale of complexity of the possible solutions; they do not depend on physically or logically centralised aggregation. Neither solution, as presented, meets all the basic user requirements or overcomes all legal and technical obstacles.

### *5.2.2 De-duplication*

Duplicates might result from the concatenation of data from different TRs. Each party to a given contract might report the event (any "flow event" such as a new trade, an amendment, assignment, etc.) to two (or more) different TRs in the same or different jurisdictions. For example, Party A might report an event to a TR located in jurisdiction A and Party B might report the same event to a TR located in jurisdiction B. If data from TR A and TR B are simply combined into a single dataset without identification and remediation of potential duplicates, a record for this single event will appear in the dataset twice and distort any measures from this dataset, such as transaction volumes, exposures or positions.

This double-reporting may have been done to comply with one or more sets of local regulations; alternatively, it may have resulted from voluntary reporting and/or recordkeeping practices. For instance, when a transaction is made on an electronic trading venue with an associated TR, the transaction might automatically flow into the venue's TR, but the counterparty might also choose to report it to another TR so that it can gain a comprehensive view of its transactions through that utility.

It is challenging to eliminate duplicate transactions particularly when combining two different datasets, and even more so in the absence of data harmonisation and standardisation. Duplicates can only be removed if data are in the form of raw transaction events; if the data are already summed up into positions or otherwise aggregated, it is impossible to eliminate duplicate records because the "building blocks" of each position calculation are not known. If a global system of UTIs were in place, it could be used to match and eliminate the duplicates. If there is no effective UTI, the central aggregator may be able to develop an approach to eliminate likely duplicates assuming some accepted degree of error (for example, the user could define duplicate events as those with the same counterparties, same contract terms, and same transaction date and times), if the dataset records are named or partially anonymised. If the dataset is fully anonymised, i.e., no counterparty information is provided, the likely volume of errors in the removal of duplicates greatly increases.

## 5.3 Principles of data management to facilitate proper data aggregation

Effective data management is a critical component of any data collection, reporting and aggregation framework. Accurate and useful data aggregation requires sound data management principles, including the following:

- Regarding the underlying data:
  - Integrity and traceability
  - Data quality
  - Standardisation and harmonisation
  - Availability.
- Regarding the technological arrangements:
  - Scalability
  - Flexibility
  - Business continuity
  - Security.

### *5.3.1 Data integrity and traceability*

From the perspective of the data aggregation of trade reports, data integrity can be defined as ensuring that the processing involved in the aggregation:

- does not distort or misrepresent the data that were originally reported,
- protects the data from unauthorised changes,
- properly represents the underlying data, without adding to or subtracting from them, in the results of the aggregation.

The concept of integrity also depends on the chosen aggregation model and must therefore remain flexible and be adapted to each particular model:

- under Option 1, the aggregation mechanism needs to store and manage its data properly,

- under Option 2, the aggregation mechanism needs to maintain the integrity of the centralised index,
- under all the options, model integrity would require consistent communication between entities.

The ability to track the history of changes to content and location of data from their inception to disposal is the primary characteristic of traceability. When collecting data for the purposes of aggregation, data quality is enhanced when the origin of data, the reasons for any changes, and those responsible for any changes to the data are known. While the primary responsibility for most of the changes to the data rests with the TRs, in cases where the aggregation mechanism makes changes to data such as anonymisation or masking, maintaining that audit trail would be the responsibility of the aggregation mechanism.

### *5.3.2 Data quality*

A discussion of the dimensions of data quality can be found in Appendix 3.

### *5.3.3 Data standardisation and harmonisation*

#### *Data standardisation*

Data standardisation is a necessary tool for effective high quality aggregation under each aggregation approach. It would be critical to determine which of the data being reported to TRs need to be collected, reported and stored in a sufficiently consistent and standardised form so that the data can be easily and accurately aggregated for the necessary uses.[38] Data standardisation also must address the potential need in some cases for authorities in their financial stability analysis to aggregate OTC derivatives data with other data, such as data gathered from other sources, on other types of trades (e.g., exchange-traded derivatives or cash market trades), and reference data, particularly references that define the products traded and identifiers for their underlying instruments or entities. In many jurisdictions reporting requirements oblige TRs to provide a specific set of data elements to regulators. At the time of this report, not all relevant legislation and regulation has provided specific instructions as to the format and content of the data elements to be reported. Some have only given an economic definition, leaving it to the discretion of the TRs to define those fields from a technical point of view. Where specific requirements are given, these requirements sometimes differ between jurisdictions. For example, currently ESMA rules require the collection of data on collateral while CFTC rules do not. Authorities must resolve these differences and agree to new or harmonised data standards and formats so that complexity in the aggregation process at the jurisdiction and global levels can be avoided or reduced.

Data standardisation is required throughout the "data supply chain" to drive efficiency up and costs down. The following highlights the key OTC derivatives data elements requiring standardisation:

[38] It is not intended to suggest that this means that the other reported data can be of lower quality, only that these are the key items necessary to make aggregation work.

*Counterparty identifier*

The counterparties to derivative transactions could be either legal entities or natural persons. The need for standardisation primarily applies to de jure and de facto legal entities, which should rely as much as possible on the LEI (see Box 2 in Chapter 4). This report does not propose requiring standardisation of the identifiers for natural persons, as data that enable the identification of natural persons are not envisaged to be included in the aggregation mechanism.

*Product identifier/ product identification system*

An international product classification system for OTC derivatives would provide a common basis for describing products, as described in the Data Report. Without a shared taxonomy the aggregation of data might be impossible or at best extremely difficult. A standardised way of identifying the product traded will enable the identification of instances where reports relating to the same product are made to multiple TRs, the identification of pockets of risk on specific products, and comparisons of trading on related, but not identical, products.

However, the standardisation of the depiction of financial products/instruments/contracts across markets and geographies has lagged behind the development of counterparty identifiers (i.e. the LEI).

The requirements for product identification in order to achieve the objectives of data aggregation are:

- An identifier that is sufficiently precise for the purposes of the authorities using the data, although recognising that it may need to be supplemented by other reported data on the transactions.
- An identifier that either explicitly or implicitly (through reference data) includes a well-articulated and precise classification hierarchy, so that data aggregation and analyses that does not require precise detail of the traded product are possible.
- An identifier that is open-source, available to all users and has open redistribution rights.
- A governance process for adding new values to the identification system, recognising that new products will come into being over time. Authorities should have some role in the governance process.
- An identifier that incorporates an approach that allows for historic data comparisons in a straightforward way, e.g. by not deleting or mapping old values. The approach would maintain a version history of the identifiers.

Several approaches have been put forward in the area of OTC derivatives product classification. These include approaches based on existing international standards (e.g. CFI Codes – ISO 10962 and ISO 20022 financial data standard) and industry-developed approaches (e.g., from ISDA, the Financial Industry Business Ontology, algorithmic contract type unified standards).

For the purposes of aggregation, it would be best if all jurisdictions select the same approach. If this cannot be achieved, then it should be possible to translate the various approaches used at the reporting level into a common approach for integration.

*Transaction/trade identification*

OTC derivative transactions may be reported to a number of different TRs and can, over their life, experience multiple amendments, notations and risk-mitigating exercises.

If there is no standardisation of the trade identifier, but instead different jurisdictions or different TRs use their own approaches, there could be problems in the areas of: (i) double-counting if transactions are reported to different TRs; (ii) linking transactions when a life cycle event occurs and different events are reported to different TRs; and, (iii) difficulty in linking an original bilateral transaction to the resulting cleared transactions.

Attempts to match up reports using other fields (such as the participants involved and/or the time of trade) without some version of the UTI concept are relatively complex, inefficient and inaccurate and not suitable for effective aggregation.

Like the product identifier, the standardisation of transaction identifiers across markets and geographies has lagged behind the development of the LEI. While some jurisdictions have implemented authority-specific transaction identifiers, there is no global standard in place at the time of this report. There are also some jurisdictions that have no authority-specific transaction identifier.

***Data harmonisation***

In the absence of full data standardisation (meaning every data element is standardised), reported data would need to be harmonised in order to ensure comparability. The term "harmonisation" can bear different meanings depending on the chosen aggregation mechanism and the envisaged use of aggregated data. Harmonisation is understood here as the process of adjusting differences and inconsistencies among different systems, methods or specifications in order to make the data derived from those systems mutually compatible.

Harmonisation is required for fields where no standardisation has been agreed on. There are some proposals to develop a translation mechanism that will permit the aggregation of data originally provided in different formats. However, such a translation is not just a matter of format, since the content of the data fields might also require translation. Standardisation arrangements such as those discussed above apply to only certain key data elements. Harmonisation of fields would be critical under any option to achieve useful aggregation.

While many vendors and technologists propose their own translation mechanisms or tools to aggregate data in disparate data stores and formats, such aggregation is prone to significant margins of error. While it might be helpful to provide initial leads for surveillance or enforcement activities such a technology is not a good substitute for standardisation of data to report the same data elements across the globe. Where complex datasets such as those dealing with OTC derivatives data are concerned, such methods could have higher rates of failure. In addition, many of these also require investments to develop data dictionaries and intermediate translation standards in order to work. So, the costs of standardising data at the source may be well worth bearing, when set against the long-term benefits for decades to come.

### *5.3.4 Availability*

Data must be present and ready for immediate use and aggregation. Under any of the options presented, there is an operational risk that the data may not be present and ready for use when

needed for aggregation. Market participants must deliver the data to TRs in time to allow the TRs to complete their processing cycle with final delivery or availability to authorities. Local and global authorities have different deadlines for reporting, holiday calendars, and operating hours. In the global context, there is no "end of day" for TRs, only specified times on a 24-hour clock by which data must be available to each authority served.

- In the case of Option 1, the availability of data at report/ aggregation time becomes the responsibility of the aggregation mechanism, with the TRs responsible for providing the necessary data ahead of time.
- Under Option 2, both the aggregation mechanism and the TRs have to be responsible for availability at report/aggregation time, since both the catalogue/ index and the source data would be necessary to achieve desired results.
- Under Option 3, most of the responsibility for availability rests with the TRs.

### *5.3.5 Scalability*

Scalability is the ability of a system to continue operating at a required level of performance as the size or volume of data processed increases. The system must be able to provide the same level of response time to queries whether the aggregation is for a single TR or across multiple TRs. As jurisdictions and TRs join in the global collection of derivatives data, the system must be able to grow to accommodate the increased volume of data collected, queries submitted, and reporting required, maintaining at the same time its performance characteristics (e.g. response time, service availability). Beyond the collection and distribution of data, aggregation requires the raw processing power to perform calculations, respond to queries, and generate the reporting that is the reason for collecting the data.

Under Options 1 and 2, the system must be able to service large numbers of simultaneous users on a global 365x24x7 basis (or whatever frequency and timeliness are specified for reports and data requests). Specifically under Option 1, there is a greater burden on securely receiving, storing and serving up large amounts of data. Under Option 2, and to some extent under Option 3, there is a greater burden on communications, multilateral data exchange, and the ability to locate data resident in distributed databases in a timely fashion.

### *5.3.6 Flexibility*

Flexibility is the ability of a system to adapt to changes in requirements or processing demands. Aggregation requirements will vary based on the regulatory or supervisory mandates of the users of the system. The system must be able to adapt to the diversity of requests and rapid evolution in queries as users become more sophisticated in their understanding of system capabilities and the data available. The system also requires the ability to adapt to new instruments, transactions, and the data storage they require.

With experience, end-users will look at aggregation in different ways, with more complex queries, and demands for greater access to data. Under Options 1 and 2, the aggregation mechanism has the responsibility to service the end-user regardless of the location of the source data. Under Option 3, the distribution of the TRs and authorities will result in lower flexibility as each system is subject to differing requirements that drive independent evolution. In addition, each requesting authority and each TR or authority providing data may

have to deal with a wide variety of data standards, formats and data transfer protocols and mechanisms, based on the number of requesters and providers.

### *5.3.7 Business continuity*

Business Continuity is "the capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident". Business Continuity Management (BCM) is "the holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities."[39]

BCM needs to look beyond IT technical recovery capability and into a more comprehensive recovery of the business taking into consideration: (i) reputational risk; (ii) data supply chain (including TRs, connectivity, etc.); (iii) communications; (iv) sites and facilities; (v) people; (vi) finance; and (vii) end-users.

The above should be considered against the changes to the environment in which the aggregation mechanism operates including political, economic, technological, social, legal, security, natural disasters, taking into account crises and incidents that might disrupt the aggregation mechanism's ability to deliver the services. The aggregation mechanism needs to exhibit network stability. It should plan for both short-term service interruptions (generally caused by technical issues) and severe service interruptions (generally caused by larger events outside the control of the aggregation mechanism and jurisdictions). The latter might require the activation of an alternative site.

Option 1 offers the possibility to manage the continuity of service in a single location, but emergency procedures (e.g. disaster recovery) need to be implemented in order to avoid single points of failure. Moreover, cases of unavailability of a single TR may introduce data completeness and timeliness issues.

Option 2 requires TRs to be always appropriately available in order to ensure required access. Cases of unavailability of data from a single TR may produce inconsistencies and hamper the possibility of receiving complete information leading to incomplete or incorrect results(especially for *ad hoc* requests).

Option 3 requires TRs and individual authorities to be appropriately available, but there are no demands on availability from a central aggregator or global perspective.

### *5.3.8 Data security*

Data security is a comprehensive approach that includes the following:

- Availability / Accessibility – information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from or prevent failures;

[39] Source ISO22301:2012.

- Confidentiality – information is observed by or disclosed to only those who have a right to know;
- Integrity – information is complete, accurate and protected against unauthorised modification;
- Authenticity and non-repudiation – data source can be trusted.

Achieving data security requires alignment of IT security with business security. Global TR data aggregation necessitates the development of a security policy for the 'end-to-end' environment, which incorporates the control of the use of the data at the TR and at the aggregation mechanism.

Data security within the 'end-to-end' environment needs to consider technical security as well as environmental security. It is also important for the aggregation mechanism to be able to have preventive, detective and reactive practices with respect to security incidents (cyber-attacks, computer crime etc.).

Under Option 1, high-reliability tools and procedures for managing centralised access to the data would need to be developed/ implemented at the central aggregator, including the choice of a secure location. This model requires the implementation of a robust security system to ensure the confidentiality of data stored in the central aggregator and the ability to centralise security checks on the stored data.

Under Option 2, data security would need to ensure secure access by the central index to the databases of different TRs and the protection of the confidentiality of local caches, which could include subsets of actual TR data. Also in these cases it will be necessary to establish secure and reliable network protocols. In the case of direct access from authorities to TRs, bilateral agreements and technical solutions need to be put in place.

Regardless of whether Options 1 or 2 is chosen, the aggregation mechanism has to have a governance function, which would manage and implement the data access rights of different authorities. The governance function itself would need to have a clear audit trail of its own actions as well as to manage a strong framework of accountability to the authorities. The governance function would need to conduct internal audits to ensure adherence to its operating practices and principles. In addition establishing the governance mechanism, TRs and the central aggregator would need to secure the communication mechanisms that move data among TRs and the central aggregator.

Under Option 3, data security becomes the responsibility of the individual TRs and authorities that access the data. Each set of authorities and TRs would need to manage their mutual access rights.

# 6. Assessment of Data Aggregation Options

This chapter provides an assessment of the pros and cons of each option on the basis of the criteria and principles discussed in Chapters 3, 4 and 5. It also considers the impact of differing levels of comprehensiveness of service in the implementation of Options 1 and 2 on the extent to which the data aggregation would fulfil authorities' mandates, as well as on the legal, data and technology challenges. Finally, while the report does not attempt to estimate

the costs of the different aggregation options, some preliminary qualitative considerations on the key drivers of costs are provided.

## 6.1 Criteria used for the Assessment

On the basis of the analysis presented in Chapters 3, 4 and 5, a list of criteria to assess the different options has been derived from the perspective of uses, legal, data and technology considerations. This list consists of a set of key aspects and requirements for the aggregation mechanism:

***Uses***

- *Scope of data needed*: as described in Chapters 1 and 3, authorities require access to aggregate data at different levels of depth, breadth and identity to fulfil their mandates. The ability of the aggregation mechanism to meet the scope of data needed in terms of breadth, granularity, identity, and ability to prevent double-counting would be one set of criteria.
- *Use flexibility*: as noted in Chapter 3, the scope of authorities' data requirements vary by mandate and the desired deliverables may evolve over time. This calls for an aggregation mechanism providing ease of use and flexibility to meet requests that evolve as financial markets and products evolve.

***Legal***

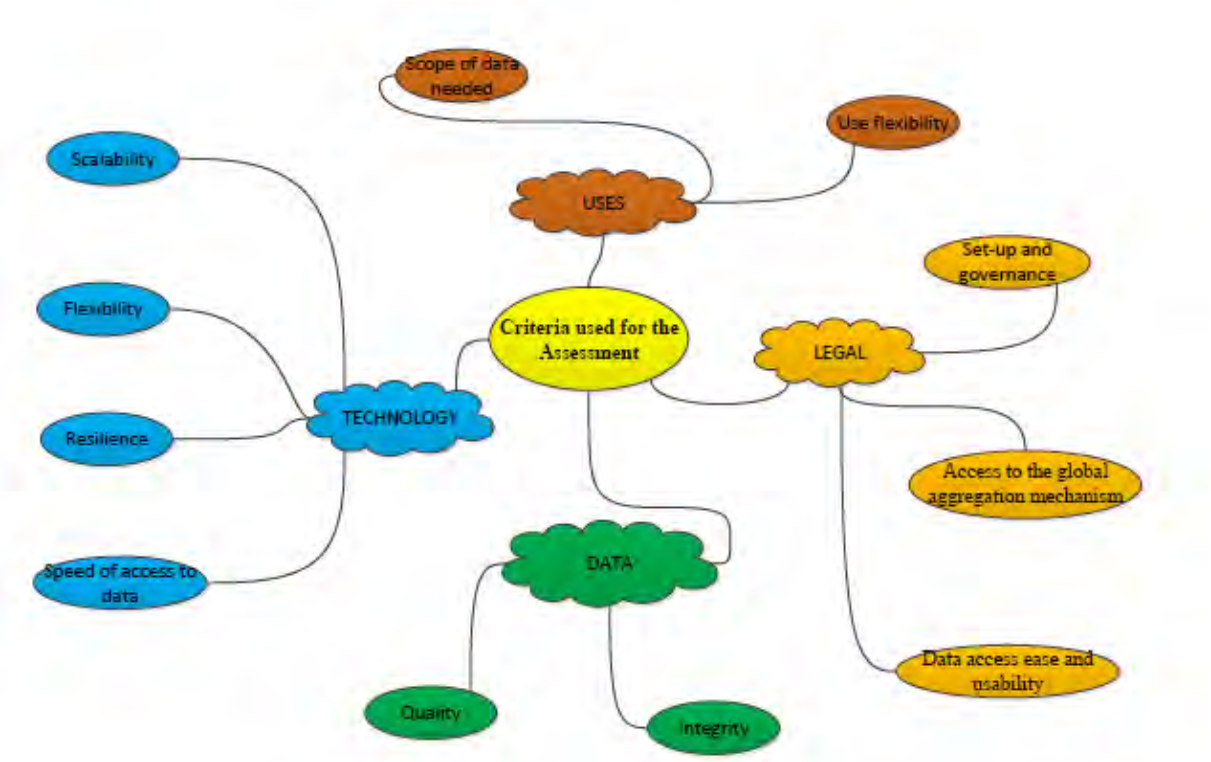
- *Set-up and governance:* given their difference in nature, the various aggregation options do not require the same steps for their creation. The aggregation options are therefore analysed in terms of the legal prerequisites and governance necessary to enable the collection of data, including confidential data, from TRs,
- *Access to the global aggregation mechanism:* in terms of governance, including for storage of data and information sharing.
- *Data access ease and usability:* given their difference in nature, the aggregation options do not provide the same level of usability to the end-users in terms of the legal steps required to access the data. The aggregation options are therefore analysed in terms of their use once the above set-up prerequisites have been established.

***Data***

- *Data quality and integrity:* in order to ensure a meaningful aggregation and subsequent analysis, the data subject to aggregation should be of high quality. Data quality dimensions considered in this report are completeness, accuracy, timeliness, consistency, accessibility and de-duplication. It is also important for the aggregation mechanism and processes to ensure that the data is complete, accurate and protected against unauthorised modification. Aspects to consider are ability to implement data integrity and risks to data integrity.

***Technology***

- *Scalability:* the aggregation mechanism should have the ability to scale to accommodate growth in scope and load and in order to manage capacity. Scalability dimensions considered include functional, processing power, data transfer and storage.
- *Flexibility of technology:* the aggregation mechanism should be evolutionary with flexibility embedded in the system to possibly cater for new aggregation requests, changes in trading behaviour or products traded, or evolving technical standards.
- *Resilience:* the aggregation mechanism should be resilient to safeguard the interests of its key stakeholders. This depends on several dimensions including the IT security of the mechanism, the degree of dependencies on the network stability between a few or multiple points, business continuity arrangements and back-up solutions.
- *Speed of access to data:* the aggregation mechanism should provide authorities with access to data for both regular requests and ad hoc requests in a sufficiently timely way to meet the needs of authorities' mandates. This may include the need for rapid responses, for instance during periods of market stress.




This set of criteria is used to assess the strengths and weaknesses of the different aggregation options described in Chapter 1, considering in particular the level of complexity related to set-up and implementation of the different options. The results of that assessment are shown in the table below. The colour scheme for the table below uses green to denote instances where a particular option appears to have relative advantages over other options according to the particular criterion. The table uses red to denote instances where a particular option would not meet all the aggregation needs of all users according to the given criterion. The colours are intended to assist in interpretation of the information in the table, but cannot substitute for the more detailed assessment in the text of this report.

**Summary assessment of options against the criteria listed in Section 6.1**

| Criteria | Option 1 – physically centralised | Option 2 – federated (logically centralised) | Option 3 – local aggregation |
|---|---|---|---|
| **Uses** | | | |
| Scope: breadth / concatenation | Global data on all counterparties, products and transactions are available through the aggregation mechanism and delivered according to individual authorities' mandates. | | Data are available from a limited set of TRs where access has been configured by each authority. Difficult to determine where required data are located. |
| Scope: granularity | There may be a trade-off between enhanced harmonisation of data and preserving the detail available in individual TRs. But this can be avoided through careful design of the aggregation mechanism. | | Potential access to all details available about data in the individual TRs. |
| Scope: ability to prevent double-counting | Duplicates can be removed before further analysis or any required anonymisation is performed, as long as aggregator receives named data or masked data. | | Duplicates can only be removed by an authority if the authority's mandate allows it to receive named data. |
| Scope: ability to provide anonymised data where required | Can provide data with anonymisation and masking (with consistent identifiers across the dataset) as required for some authorities mandates, as long as aggregator receives named data. | | Cannot provide data with consistent masking of counterparty identifiers at the global level as required for some authorities' mandates. |
| Use flexibility: ease of use | Provides single point of entry for authorities to obtain consistent and harmonised data. | | Analysis must be customised to each TR. The data sourced from separate TRs would need to be harmonised by each authority that needs to create aggregate-level data. |

| Criteria | Option 1 – physically centralised | Option 2 – federated (logically centralised) | Option 3 – local aggregation |
|---|---|---|---|
| Use flexibility: new products and evolutionary requests | Requires a flexible governance structure to avoid slowing the submission of new analytical queries and a flexible database (for Option 1) or data retrieval (for Option 2) setup. | | • Each authority can decide how to use raw data provided by TRs.<br>• But each authority would have to cope separately with each change to data structure or fields made by any TR. |
| Use flexibility: frequency of data updates | Authorities could request data updates at any time, but the timeliness of data is determined by the update loading cycles of the aggregator. | Authorities could request data updates at any time, but must wait for data retrieval process (between the aggregator and the TRs) to complete. | Authorities could make requests to TRs at any time, but must wait for data retrieval process (including any needed prior aggregation process) from each TR to complete. |
| **Legal** | | | |
| Set-up and Governance | *The set-up of Options 1 and 2 relies on a multilateral framework that does not exist yet. In most jurisdictions, the set-up of such framework may require amending existing laws beforehand.* | | *The set-up of Options 3 relies on existing frameworks. It may be immediately implemented in the majority of jurisdictions where TRs are established. However, in the absence of a multilateral framework, its implementation requires the conclusion of multiple bilateral agreements. It also requires amending existing laws where access to TR data is not currently possible.* |
| | Options 1 and 2 may not be immediately implementable in the existing legal environments. | | In most jurisdictions, existing laws allow a foreign authority to access data held in local TR subject to certain conditions being met. However, in some jurisdictions, existing laws would have to be amended where foreign access to TR data is not currently possible. |
| | • The implementation of Options 1 and 2 requires agreeing on, and setting up, a multilateral institutional framework governing the aggregation mechanism (in particular, specifying (i) the entity responsible for operating the global aggregation mechanism, (ii) the | | The set-up of Option 3 requires, as a prerequisite, pre-conditions being satisfied (e.g. conclusion of international agreements/cooperation arrangements/MoUs) or addressing existing obstacles (e.g. indemnification provision). |

| Criteria | Option 1 – physically centralised | Option 2 – federated (logically centralised) | Option 3 – local aggregation |
|---|---|---|---|
| | access rules, (iii) the governance rules, etc.).<br>• The set-up may prove more complex than relying on existing bilateral frameworks. However, once in place, the governance framework may have fewer complexities. | | |
| | The governance of Option 1 would be centralised through the specification of the role and responsibility of the single central entity. | The governance of Option 2 may need additional layers to clarify the roles and responsibilities of the aggregator vis-à-vis TRs. | In the absence of a multilateral framework, the governance of Option 3 would be managed bilaterally. |
| | The set-up of Options 1 and 2 would be multilaterally negotiated – and may require a multilateral agreement (MMoU). | | The set-up and governance of Option 3 would likely be bilaterally negotiated, relying on a web of bilateral agreements. If agreements are made bilaterally, the number of agreements needed for authorities to access each other's data rises exponentially with the number of authorities involved.<br><br>Multilateral arrangements could also be envisaged to support the implementation of Option 3, albeit probably among a smaller group of authorities than envisaged under Options 1 and 2. |
| | | | |
| Access to the global aggregation mechanism | Under Options 1 or 2, it is envisaged that authorities would need to sign up once to the global framework before being permitted to access or use the data in the central aggregation mechanism, which reduce legal steps required by those authorities to access and use that data (provided that appropriate laws have been enacted). | | Under Option 3, each authority may need to sign up to multiple bilateral MOUs or other agreements before being permitted to access or use the data in TRs, which increase legal steps required by those authorities to access and use that data. |
| Data access ease and usability | The central index/aggregator may be able to provide authorities with anonymised aggregate-level data sourced from multiple TRs, which reduce legal steps required by those authorities to access and use that data. | | The requesting authority would need to obtain the data it wishes to aggregate from multiple TRs, making the process for access to the data more difficult and time consuming for the requesting authority. |

| Criteria | Option 1 – physically centralised | Option 2 – federated (logically centralised) | Option 3 – local aggregation |
|---|---|---|---|
| **Data** | | | |
| Enforcement of data quality and integrity | The operator of the central aggregator can coordinate the development of data quality measures and metrics. However data quality of the source TR data will need to be high regardless. | | The regulators and TRs must coordinate and agree among themselves on the development of data quality measures and metrics. |
| **Technology** | | | |
| Scalability | Users can access any number of TRs through a single point of entry. | | Users may need a new connection and potentially new protocols for each new TR or authority. |
| | The central hub must provide additional storage and computational power on an as-needed basis. This means designing for peak loads and providing excess capacity for expansion without interruption of services. Scalability is a shared responsibility of the central hub and the TRs. | The central aggregator index does not need to provide for local storage (other than storage for the index and temporary storage to handle queries in progress) but must be able to scale its network and computational resources. Each TR provides expansion capability based on the business strategy of the repository operator (which might need additional alignment with global aggregation needs). | Each TR provides expansion capability based on the business strategy of the TR operator. Scalability is thus the responsibility of each TR individually. |
| Flexibility of technology | Changes to database required to add the data for new products and collect the data in new ways may be challenging. | Retrieval process can be adapted to new requirements. The technology solution must be designed to minimise the impact on response time of new requirements. | Authorities have the flexibility to access raw data as required, but building new processes would be very challenging. |

| Criteria | Option 1 – physically centralised | Option 2 – federated (logically centralised) | Option 3 – local aggregation |
|---|---|---|---|
| Resilience | Central storage provides a backup to data stored in TRs, allowing authorities to access data in the event of a TR failure. The central hub must provide the ability to withstand failures and outages both locally and among the distributed TRs. | Access to data would be interrupted if either the central aggregator or a TR were inaccessible. The aggregator needs to be able to provide partial data in the event of TR failure. Because the costs of such resilience must also be borne by the individual TRs, it is likely to have an impact on them. In addition, system-wide costs could be higher than setting up resilience for a single location. | The distributed repositories must provide the ability to withstand local failures and outages. |
| Speed of access to data | Data is pre-processed and readily available for authorities | Data retrieval process (between the TRs and the aggregator and then between the aggregator and the authorities) is likely to take longer than in Option 1. | Retrieval and processing of raw data involving several TRs would likely take more time. |

## 6.2 Assessment of varying degrees of comprehensiveness of service in the implementation of Options 1 and 2

In setting up an aggregation mechanism, authorities will be faced with the challenge of deciding the extent of services to be provided by the central aggregator to authorities. Versions of the aggregation mechanism offering less comprehensive service might be less complex and less costly to set up. But less comprehensive versions may only meet some uses across the mandates detailed in the Access Report, and in some cases may have no advantages in terms of complexity and cost.

A range of such choices of service level is possible. This section considers the impact of varying the level of service required from the mechanism, across the five dimensions of how data can be aggregated and presented that are described in Chapter 1, i.e. depth, breadth, identity, coverage, and degree of manipulation. For simplicity of analysis, the discussion below considers each dimension in isolation. The analysis focuses on the impact for Options 1 and 2. Since Option 3 does not have a central aggregation mechanism, this analysis does not apply to Option 3.

Variations in the level of service required would impact authorities' ability to fulfil their mandates, as well as impacting the legal, data and technology challenges. To illustrate the impacts on authorities' ability to fulfil their mandates, this section focuses on three "use cases" – selected from among the mandates described in the Access Report – which are representative of the various data needs of authorities and which may be affected by the level of service that the aggregator can provide. The three use cases are:

- *Monitoring of sectoral and geographic aggregates:* this use case would involve tracking broad trends in derivatives markets. These trends may highlight any significant risk transfer between institutional groupings based on geography and/or economic sector. (On identifying a significant transfer between groups, an authority might wish to see more granular data relating to individual institutions within the groups involved in the transfer; whether it is entitled to see the data would depend on the authority's access rights.) This use case falls under the "general macro assessment" mandate and may also contribute to the assessment of market concentration within the "systemic risk assessment" mandate described in the Access Report. Authorities currently have no source for such data on a globally aggregated basis, because it requires the ability to sum data across different TRs, including data relating to entities which the authority may not be able to access on a name-specific basis.
- *Network analysis:* this use case also belongs to the functional mandate "systemic risk assessment" in the classification of mandates of the Access Report. Network analysis allows authorities to analyse interconnectedness of entities. According to the Access Report "analysis of interconnectedness involves describing and analysing the network of links across participants within a market segment of the OTC derivatives market, and/or across different segments. It shows who the central players are, where the vulnerable links are and how the shape and characteristics of the network change over time". Authorities wanting to do this type of analysis on a global basis currently

have no source for the necessary data, as the analysis requires globally aggregated data where identities are anonymised for entities outside of their jurisdictions.

– *Conducting market surveillance and enforcement:* according to the Access Report this mandate requires authorities "to monitor market activity for anomalous trading activity, including market and price manipulation, insider trading, market rigging, front-running and other deceptive or manipulative conduct". This type of authority typically is able to access transaction-level data from TRs within its own jurisdiction and may (subject to the necessary legal arrangements) be able to access data from other individual TRs. But a single aggregated source for transaction-level data involving, for instance, domestic underliers traded both inside and outside of its jurisdiction or transaction-level data involving domestically-located entities, including their foreign branches and subsidiaries, would ease the analysis.

Overall, the analysis below shows that while a variation in the comprehensiveness of service provided, in terms of the five dimensions identified in Chapter 1, restricts the ability of authorities to conduct the overall range of tasks under the selected mandates, it mitigates only to a limited extent the legal, data and technological challenges.

-xxxxxxxxxxxxxxxxxxxxx-

**Dimension 1: Depth of the data maintained**

The Access Report defines three levels of *data depth*: transaction-level, position-level, and aggregate-level data. Transaction-level data involve records of the economic terms of individual derivatives contracts between two counterparties. Position-level data are a snapshot at a point in time of all open positions for a particular product or type of products for a given counterparty or group of counterparties. By definition, duplicate transactions have been removed before position calculations are performed. Aggregate-level data refers to data summed using various categories attributable to all participants, including by product, currency, region, underlier, etc., that are not specific to any uniquely identifiable participant or transaction.

Impact of *Depth* on use cases

Transaction-level data provides the greatest level of depth, and therefore usability, of the data. Limiting the depth of data to be maintained by the central aggregator to position-level or aggregate-level data could limit not only the possible access to the data by authorities under different mandates, but also the usability of the data for various purposes. More granular data can be transformed into less granular data; however, the reverse is not true. For example, if the central aggregator maintained transaction-level data, either the aggregator or each receiving authority – depending on the authority's access rights – could transform the information into position- or aggregate-level data as needed for each use case. An authority with a systemic risk mandate would be able to perform **network analysis**, for instance, by transforming the transaction-level data into position-level data.

But aggregate-level data cannot be broken out into position- or transaction-level data. If the central aggregator only maintained summed aggregate-level data, it would meet the needs of authorities under the "general macro assessment" mandate that wish to conduct **monitoring of sectoral and geographical aggregates**. But authorities wishing to see more-granular

position-level data after being alerted to particular trends in the aggregate-level data would have to separately collect position-level data themselves from TRs, which they could access only for institutions in their own jurisdictions or as otherwise specified under their access rights. More generally, summed aggregate-level data would not meet the need of authorities with access rights to position- or transaction-level data, for instance those wishing to conduct **network analysis** of individual institutions' positions under the systemic risk assessment mandate. It would also not meet the needs of authorities conducting **market surveillance and enforcement**, as this type of analysis requires transaction-level data. These authorities would therefore be need to approach individual TRs (assuming they have access rights) to monitor for misconduct by domestically-located institutions' foreign branches and subsidiaries, or involving transactions on domestic underliers taking place in other jurisdictions.

Impact of *Depth* on legal, data and technology considerations

From a legal perspective, submission by TRs only of summed aggregates to a central aggregator (for example as mentioned in Sections 4.1.3 and 5.2.2) may reduce legal barriers in several jurisdictions (where data that do not enable the identification of individual counterparties can be submitted by the TRs). There may also be benefits from a data and technology perspective from moving to the collection of less-granular data. Options 1 and 2 would have to store more data if position-level data were required rather than aggregate-level data and they would have to store even more data if transaction-level data were required. Although data storage costs have fallen significantly in recent years, storing large volumes of transaction-level data could have an important bearing on the cost of Option 1, because Option 1 makes copies of trade repository databases, so storage capacity would have to be of the same order of magnitude as the aggregate storage capacity of the trade repositories supplying data. In contrast, Option 2 would have relatively lower data storage costs as it would need storage only for indexing and caching. In addition, both options would need to access TR data and export information, whether to the central database (Option 1), or the central query engine (Option 2). The more granular the information that is required, the higher the specification of technology required to search for the desired information in trade repository databases and to carry the results over the internet to a central aggregator or direct to authorities.

As Option 1 collects all TR data together, it would have to carry large volumes of data over the internet if transaction-level data were required. Option 2 could avoid this partially by aggregating data 'on the fly' as TR databases are queried and only send aggregate results to the central query engine. Nevertheless, Option 2 may still need to carry a significant volume of data over the internet. For example, to ensure that queries have successfully identified trades reported multiple times, comprehensive lists of UTIs would have to be carried between TRs and the central query engine under this option. Option 2 would also need some technology at each TR to do the 'on the fly' aggregation. Both Options 1 and 2 would have to invest in technology and processes for information security and data integrity.

-xxxxxxxxxxxxxxxxxxxxx-

**Dimension 2: Breadth of the data maintained**

*Breadth of data* refers to the ability to access the data related to all counterparties or only a selected predetermined set. Aggregating data only for a selected predetermined set of

counterparties would restrict the ability of authorities to conduct analysis on the entire OTC derivative market and would prevent analysis of counterparties outside those in the selected set.

Impact of *Breadth* on use cases

Limiting the breadth of the data collected presents disadvantages; how great these would be depends on how well the authorities are able to identify in advance the most important counterparties to monitor. And, by definition, excluding counterparties prevents an examination of the whole market. Limiting the number of counterparties covered by the data would limit the effectiveness of any analysis done using that data. For **monitoring of sectoral and geographical aggregates,** it would be impossible to know whether trends in high-level aggregates or measures of systemic vulnerabilities are significantly biased, for example, without performing analysis on the counterparties outside of those in the restricted group. For **network analysis**, there would be a risk that counterparties that represented significant nodes in the network had been missed. For **market surveillance and enforcement**, authorities would need to approach individual TRs separately (assuming they have access rights) to monitor for misconduct by participants that are not among the selected set of entities.

Impact of *Breadth* on legal, data and technology considerations

There is likely little or no benefit from a legal perspective of a model where only data from selected counterparties are provided to authorities.

In terms of data and technology, enabling authorities to access only a limited pre-specified set of counterparties could add a layer of complexity due to the need for TRs to track and segregate data relating only to these counterparties. On the other hand, the operational complexity of the aggregator could be reduced because of the smaller number of firms in the sample.

Determining which counterparties to exclude would present a practical challenge. Global agreement by authorities would need to be reached on criteria for inclusion or exclusion, such as type of institution, size of institution, size of positions, size of trades executed, or frequency of trading.

-xxxxxxxxxxxxxxxxxxxx-

**Dimension 3: Identity of the counterparty**

In the most comprehensive form of the aggregator, it could provide authorities with data on named individual counterparties (where authorities are entitled to access such data). A less comprehensive variant could involve the provision of named or masked transaction-level data by TRs to the aggregation mechanism and the aggregation mechanism providing only data in an anonymised form to the relevant authorities.

Impact of *Identity* on use cases

An aggregator that was able to provide named data would need to ensure that only anonymised data was provided to authorities without access rights to the named data. This would enable authorities needing to **monitor sectoral and geographic aggregates** or conduct **network analysis**, but without access rights to named data, to do so. For **market surveillance**

**and enforcement,** authorities would be able to obtain the named data to which they have access rights**.**

An aggregator that only was able to provide anonymised data would be able to meet the needs of authorities to **monitor sectoral and geographic aggregates.** However, it would only enable network analysis to take place on the basis of anonymised network data, and would not have the capability to supply named data to authorities entitled to that data within their own jurisdiction, which would only meet the network analysis needs of those authorities that are not entitled to any named data at all. The data would not meet the needs of **market surveillance and enforcement** authorities, as market surveillance requires named data; at best it would provide indicative information for this purpose that could provide lines of enquiry for the relevant authorities to follow up by collecting named data from individual TRs.

Impact of *Identity* on legal, data and technology considerations

In terms of data and technology, enabling authorities to access anonymised data only would likely reduce the number of steps required to establish a working aggregation model. The operational complexity of the aggregator would be reduced because the aggregator would not need to create separate datasets for each authority depending on their access to named or anonymised data. A single masked dataset could be used for all authorities. (Different authorities might still require different breadth or depth of data.)

There may be little benefit from a legal perspective of a model where only anonymised data is provided to authorities, if TRs still need to provide named data to the aggregator to allow it to perform consistent masking and removal of duplicates.

If a method can be found where anonymised data can be sent to the central entity with duplicates already removed, this may alleviate some of the legal challenges related to privacy, blocking or secrecy in the setting up of the central aggregator. However, while a number of methods were considered by the study group, at some point in the process some function (even if not the aggregator itself) has to have the mapping between entity identifiers and proxy masked data. To trust such an entity with such critical information would require a robust legal and governance framework.

On the other hand, if the TRs provide named data to the aggregator, the aggregator would itself require a robust legal and governance framework to assure the TRs that the named information would be protected. The aggregation mechanism would also need to set up additional processes – coordinated with the TRs – in order to consistently mask and remove duplicates (see discussion in Chapter 5). These additional processes would increase the overall operational complexity of the aggregator and might increase the risk of masked data being inappropriately de-anonymised.

-xxxxxxxxxxxxxxxxxxxxx-

**Dimension 4: Coverage – Asset classes covered**

The coverage of the data could vary between one asset class and all asset classes. Establishing a central aggregator covering one asset class would be less complex and costly than establishing an aggregator covering several asset classes. It could be considered in a phased approach that the aggregator starts by covering one asset class and would integrate over time

other asset classes. If, as a starting point, only one asset class were to be covered, that class might be chosen either according to its relative importance for financial stability or according to the degree of standardisation of the products in the asset class. The credit derivatives or interest rates derivatives markets, for instance, might best meet these criteria.

Impact of *Coverage* on use cases

By definition, a mechanism limited to one asset class would not permit authorities to perform a comprehensive analysis of OTC derivatives markets. This would be limiting for all use cases, as authorities would only be able to use the data to **monitor sectoral or geographic aggregates** or conduct **market surveillance and enforcement** within the asset class concerned. Authorities would not be able to conduct **network analysis** that covered the overall systemic risk arising from exposures across the range of asset classes.

Impact of *Coverage* on legal, data and technology considerations

Aggregating OTC derivatives data in one, rather than all, asset classes would not impact the legal considerations analysed in the report. Indeed, the legal constraints identified earlier in this report would be likely to equally apply across all asset classes.

However, aggregating OTC derivatives in one rather than all asset classes would considerably decrease the volume of data being manipulated, which would lessen the data and technology costs of setting up and managing the aggregation system. The operational complexity of the system would also be reduced with the decrease in the size of the datasets and reduced number of fields.

Moreover, if the scope of the aggregation mechanism focuses on an asset class where products are most standardised globally, the implementation of the aggregation system would be facilitated by the already existing harmonisation of data fields and standards used for reporting (e.g. CDS or FX). In that sense, one could think of a 'pilot' project, where the global aggregation mechanism would be built to aggregate global information on, for instance, CDS only, which could be faster to implement from a data and technology point of view than a global aggregation mechanism in all asset classes.

-xxxxxxxxxxxxxxxxxxxxx-

**Dimension 5: Degree of manipulation by the aggregator**

The functionality of a central aggregator could range between offering very basic functionality to very complex manipulation and data reporting functionality. At its simplest, the central aggregator could serve as a simple pass-through of data from TRs to authorities. At the other extreme, a comprehensive central aggregator could perform technical harmonisation to ease the analysis of data, calculate metrics or other computations across TRs and provide a wide variety of aggregated data sets to authorities, based on the authorities' differing needs and access rights. In addition, the interface for the central aggregator could be very simple or comprehensive. For example, the interface might only produce standardised reports to all authorities or it could allow authorities to customise very complex data queries.

Impact of *Degree of manipulation* on use cases

The aggregation mechanism would need to have the capability to sum the data in a variety of ways in order to meet the needs of authorities **monitoring sectoral or geographic**

**aggregates**, particularly those authorities that would not be entitled to the individual transactions data in order to sum the data themselves. It would need to have the capability to transform transaction data into position data in order to meet the needs of authorities conducting **network analysis** and anonymise the data for those authorities not entitled to named data. On the other hand, authorities conducting **market surveillance and enforcement** would likely find many of their needs met by raw data**.**

Impact of *Degree of manipulation* on legal, data and technology considerations

A central aggregator with minimal functionality would entail less technical complexity and cost than an aggregator with very comprehensive functionality.

Ultimately, however, those data needs that involve complex data manipulation will need to have the complexity and cost burdens borne by TRs, the aggregator or individual authorities. As a result, a low-manipulation aggregator may itself be simpler and less expensive to implement and operate, but the costs would simply shift from the central aggregator to either individual authorities or TRs. In the case where data manipulation is shifted from the central aggregator to individual authorities, each authority would have to make parallel investments to achieve the same outcome. From a holistic perspective, this likely would be less efficient than constructing a data manipulation function within the central aggregator.

### 6.3 Cost drivers and other cost considerations

Any assessment of the costs entailed by the different options is difficult and potentially misleading at this stage since the cost depends on the expected service level, security requirements, frequency of access, number of users and data volumes, etc. A cost assessment should differentiate between initial costs and recurrent running costs, respective proportion of whose may vary considerably from one solution to another: for instance a decentralised option requires no investment at the beginning but might in the end cost more than a centralised or federated option, because of the recurring larger costs supported by the multiple users/authorities where no collective facility is available.

The discussion of costs in this report is necessarily a very high-level one for several reasons: (a) the group's mandate was to technically compare the options; (b) as stated above, more specificity is needed about several requirements in order to have a better idea of cost; and (c) the limited time available. Thus, the cost discussion in this report aims to be informative in a qualitative sense. Further work would be necessary to provide more specific details, as noted in the Executive Summary.

Appropriately centralised or federated solutions (Options 1 or 2) may generate significant economies of scale for all users. As a trade-off, these savings could be reduced by the shared cost of building and operating the centralised solution, although these costs could be different for physical or logical centralization. The cost for the different authorities should also be taken into account, including development of individual IT solutions by authorities and staff dedicated to handling data, queries and results. While its impact is difficult to quantify precisely, a lower standardisation of data would imply significantly greater costs for all users since each authority would have to spend additional time to adapt and interpret complex data sets.

A decentralised option (Option 3) would likewise entail substantial costs while potentially shifting the cost to the local level because TRs or authorities wold have to undertake data translation and normalisation at the local level in addition to developing connections and access rules for a wide range of users (while also facing greater security issues), or otherwise handle *ad hoc* requests by authorities. If authorities are required to deal manually with other authorities' requests, this would similarly entail additional costs, including staff that would need to be dedicated to this task to complete the request on individual basis in differing formats and protocols.

Centralised or federated solutions entail specific costs that can be distinguished into initial cost and running cost, and that should be considered from the perspectives of all the affected entities (authorities, central facility, TRs). Initial costs include mainly:

- Infrastructure and hardware (storage, network),
- Software (extranet, security, connection to users and access rights initialisation),
- Physical location,
- Data (standardisation, harmonisation),
- Project design and management (governance design, IT design, legal).

Running costs mainly include:

- Infrastructure and hardware (storage, network, system updates and improvements, maintenance, processors and main memory),
- Software (extranet, security, connection to users and access rights management),
- Facilities (Physical location),
- Staff (executive team and management, business operations (data handling and analysis), system operations and technology, finance / admin / HR / facilities),
- Legal.

These potential costs should be set against the large opportunity cost if the chosen solution does not allow for an optimum use of worldwide TR data or if the effort for accessing the data is too high.

Given the high-level nature of the study, this report has not been able to quantify the costs of the various options. However, it has conducted a qualitative study into the cost drivers and cost categories that would be expected to apply. This has led to the following findings:

1. The initial set-up costs of either Option 1 or 2 are likely, from a global perspective and including the set-up costs incurred by individual authorities, to be less expensive than for Option 3. The main reason why Option 3 is likely to be more expensive than the other options is the need for multiple authorities to build similar aggregation processes, in order to deal with differences between the TRs and to have to link to multiple TRs rather than having an aggregation mechanism do this once and sharing the service among the community of authorities and TRs. Options 1 and 2 both avoid these issues. The initial costs for Options 1 and 2 arise in different ways (Option 1, for example, needs far more central storage than Option 2, while the design of

Option 2 is thought to be more complex), but it is not possible to determine at this stage which is likely to be relatively less expensive.

2. The picture might be comparable for the ongoing operating costs. Again, from a global perspective, Option 3 is likely to be more expensive in total than either of the other two options because it does not allow authorities to leverage the synergy of centralised functions. Again, there is little to choose between Options 1 and 2 when considered solely from the cost point of view. However, Option 1 is likely to be slightly more expensive than Option 2, as Option 2 would primarily incur operating costs when used by authorities for requests, while Option 1 would have to be fully operable, even at times without any request activity.

3. The other difference in cost terms between the options is the question of which type of stakeholder (i.e. central aggregator or user authorities) would directly bear the costs, although it has to be stressed that the analysis in this report does not address the question of how the costs of the central aggregator might ultimately be allocated. In the case of Options 1 and 2, the main cost centre would be the central aggregator. Between Options 1 and 2, it seems likely that Option 1 would centralise more of the cost on the aggregation hub compared to Option 2, which tends to distribute more of the costs amongst the other stakeholders. In Option 3, most of the cost is incurred by, and therefore distributed amongst, the authorities accessing the data, according to the scale and complexity of their usage; under this option, each authority can independently decide (through their level of usage) the costs they incur.

4. Generally speaking, the development of a shared infrastructure should lead to overall savings in the cost of development and management for authorities compared to the case in which each authority would develop aggregation capability on its own. However, it should also be recognised that, even once a shared infrastructure is in operation, some authorities may, to a greater or lesser extent, also collect and aggregate data directly from TRs in support of some or all of their mandates. This duplication of costs between localised and shared infrastructure would offset some of the benefits from economies of scale.

# Appendix 1:
# Feasibility study on approaches to aggregate OTC derivatives data

**Terms of reference**

**22 July 2013**

## I. Introduction

G20 Leaders agreed, as part of their commitments regarding OTC derivatives reforms to be completed by end-2012, that all OTC derivatives contracts should be reported to trade repositories (TRs). The FSB was requested to assess whether implementation of these reforms is sufficient to improve transparency in the derivatives markets, mitigate systemic risk, and protect against market abuse.

A good deal of progress has been made in establishing the market infrastructure to support the commitment that all contracts be reported to trade repositories. As noted in the FSB's April 2013 OTC derivatives progress report[1], at least 18 TRs have been established to date, located across ten jurisdictions, with some intended to operate internationally and others purely domestically. However, further study is needed of how to ensure that the data reported to TRs can be effectively used by authorities, including to identify and mitigate systemic risk, and in particular through enabling the availability of the data in aggregated form.

The CPSS-IOSCO consultative report on authorities' access to TR data, published on 11 April 2013[2], notes that:

> *"With the current structure of TRs, no authority will be able to examine the entire global network of OTCD [OTC derivatives] data at a detailed level. In addition, it is likely that OTCD data will be held in multiple TRs, requiring some form of aggregation of data to get a comprehensive and accurate view of the global OTC derivatives market and activities. Absent that, the financial stability objectives of the G20 in calling for TRs might not be achieved.*
>
> *In light of these limitations, the opportunity for a centralized or other mechanism to provide global aggregated data, as a complement to the direct access by the different authorities to TR held data, probably warrants consideration and further investigation, although beyond the scope of this report[3]".*

---

1 Available at http://www.financialstabilityboard.org/publications/r_130415.pdf

2 Available at http://www.bis.org/publ/cpss108.pdf

3 The CPSS-IOSCO report text added the following here in a footnote:

"For performing macro assessments, or supporting provision of data for systemic risk analysis, it is probably worth investigating the feasibility of how a centralised or other mechanism would be able to collect position level and transaction level data from TRs globally and aggregate, summarise and ensure anonymity of the data, subject to applicable local law. The granularity of data could entail breakdowns by jurisdictions and counterparty types.

The FSB's April 2013 OTC derivatives progress report follows up on this suggestion by recommending that further international work should take place on:

> *"the feasibility of a centralised or other mechanism to produce and share global aggregated data, taking into account legal and technical issues and the aggregated TR data that authorities need to fulfil their mandates and to monitor financial stability."*

Achieving global aggregation of data may involve several types of aggregation of transaction data: within individual TRs, across TRs and across jurisdictions. To successfully produce and share globally aggregated data, the following elements would need to be addressed to achieve successful aggregation of the TR data to meet regulatory objectives:

- definition of the data to be aggregated;
- sufficient standardisation of data formats to enable aggregation;
- reconciliation of data (for instance, to avoid double-counting and gaps);
- establishment of a mechanism(s) for the production of data in aggregated form, supporting the availability of summarised and anonymised data where relevant; and
- provision of access to authorities as appropriate.

The feasibility study will build upon and take forward the previous work done by other groups, including the January 2012 CPSS-IOSCO report on OTC derivatives data reporting and aggregation requirements[4] and the April 2013 CPSS-IOSCO consultative report on authorities' access to trade repository data.

## II. Objectives of the study

The feasibility study should set out and analyse the various options for aggregating TR data. For each option, the study should:

- set out the steps that would need to be taken to develop and implement the option,
- review the associated (and potentially interdependent) legal and technical issues, and

---

Such a mechanism could support making the data available to all relevant authorities in standardised reports on a regular basis, that would parallel and could learn from, for example, the international financial statistics or the OTCD survey data. It could also facilitate publication of a set of aggregate data."

[4] The January 2012 CPSS-IOSCO report stated: "Work to develop a standard product classification system for OTC derivative products is needed as a first step towards both a system of product identifiers for standardized instruments and an internationally accepted semantic for describing non-standardized instruments. The Task Force recommends that CPSS-IOSCO or the FSB make a public statement calling for the timely industry-led development, in consultation with authorities, of a standard product classification system that can be used as a common basis for classifying and describing OTC derivative products. Therefore, the Task Force recommends that the FSB direct, in the form and under the leadership the FSB deems most appropriate, further consultation and coordination by financial and data experts, drawn from both authorities and industry, on a timely basis concerning this work."

- provide a description of the strengths and weaknesses of the option, taking into account the types of aggregated data that authorities may require and the uses to which the data might be put.

The information and technical analysis in the study will provide an important input to assist senior policy-makers in their decision on whether to initiate work to develop a global aggregation mechanism and which form of aggregation model should be used.

The options for aggregating TR data to be explored by the study include:

1. A physically centralised model of aggregation. This typically involves a central database (hub) where all the data are collected from TRs, stored and subsequently aggregated within the central database for onward provision to authorities as needed.
2. A logically centralised model of aggregation based on federated (physically decentralised) data collection and storage. Logical centralisation can take a number of forms but the key feature is some type of logical indexing mechanism that enables the use of technology to aggregate data from local TR databases rather than the use of a physically central facility. In this option the underlying transaction data remains in local TR databases and aggregated with the help of the central index (using pointers to local databases). One variant of logical centralisation is a model where the data is collected and stored locally but, instead of authorities using the logical indexing mechanism themselves to obtain the data from local databases, there is a designated agent that maintains the central index and the platform for responding to requests from authorities.
3. Collection of raw data from local TR databases by individual authorities that then aggregate the information themselves within their own systems.

Other aggregation models could also be explored, as the study group considers appropriate.

## III. Components of the feasibility study

The feasibility study should begin with a brief stocktake of the current use of TRs for reporting of transactions, including the number and location of TRs as well as utilized data reporting templates and standards, so as to provide information on the current state of the distribution of TR data that would need to be aggregated. The stocktake should draw wherever possible on existing information on current availability and use of TRs (for instance in the FSB's OTC derivatives progress reports and the information collected through CPSS-IOSCO monitoring of the implementation of PFMIs). The stocktake should also incorporate information (where known) on additional TRs that are planned but not currently operational, and of the likely implications of reporting requirements that are still under development in several jurisdictions for the use of TRs. This brief stocktake will be needed in order to provide some background on the scale and scope of the aggregation challenge.

The study should then address the following interrelated issues for each aggregation option set out above: achievement of the high data quality and consistency that authorities need from aggregated data, including appropriate data standardisation requirements and reconciliation mechanisms; data access and associated legal issues (including anonymisation of data where relevant); and the analysis of technical, organisational, operational and implementation issues

associated with each model. (The ordering and length of description of each issue below is not intended as an indication of the relative importance and amount of the work to be done in the feasibility study.)

**III.1 Quality and consistency of data including appropriate data standardisation and reconciliation**:

It is difficult to aggregate data (within a single TR and across TRs nationally or globally) without consistent definition and representation of the data elements to be aggregated. This consistency could be achieved either in the initial reporting of transactions to TRs or through translation of the data into more globally consistent representations during the aggregation process.

The study should make an initial analysis of the extent to which aggregation would be possible with the data that will be available under current reporting requirements to TRs. It should identify possible obstacles to the ability to globally aggregate data that may arise from the gaps, inconsistencies or incompatibilities in the data fields, definitions or formats that market participants report to TRs. Identifying the current scope for aggregation and the obstacles will require an initial stocktaking of data field requirements and definitions and data formatting requirements in multiple jurisdictions, including whether these requirements are codified in law or regulation.

The study should also analyse what would constitute a core set of OTC derivatives data elements that, if available in sufficiently standardised form, would enable the aggregation of data among TRs to support regular monitoring as well as other types of analysis by authorities, including of systemic risks. (Such a core data set could then be expanded over time if necessary.) The study should also consider possible approaches to standardising that data.

In this regard, the study should draw upon recommendations in the January 2012 and April 2013 CPSS-IOSCO reports and also the work of the FSB's OTC Derivatives Data Experts Group (ODEG), which considered the data needs of the official sector users of OTC derivatives data. Although the study's analysis would be directed at standardisation needs in relation to establishment of a global data aggregation mechanism, it may also be relevant to recall a recommendation of the January 2012 report that, in addition to the creation of a system of legal entity identifiers (LEIs), international work be undertaken to develop an international product classification system for OTC derivatives to provide a common basis for describing products.[5]

The study should also analyse approaches (whether through data standards, reporting guidelines, or otherwise) to avoid the double-counting of transactions through the aggregation process which might arise where transactions are reported to more than one TR or reported

[5] The January 2012 CPSS-IOSCO report stated: "Work to develop a standard product classification system for OTC derivative products is needed as a first step towards both a system of product identifiers for standardized instruments and an internationally accepted semantic for describing non-standardized instruments. The Task Force recommends that CPSS-IOSCO or the FSB make a public statement calling for the timely industry-led development, in consultation with authorities, of a standard product classification system that can be used as a common basis for classifying and describing OTC derivative products. Therefore, the Task Force recommends that the FSB direct, in the form and under the leadership the FSB deems most appropriate, further consultation and coordination by financial and data experts, drawn from both authorities and industry, on a timely basis concerning this work."

more than once to the same TR (for instance because both counterparties to a transaction separately report the transaction).

Among the questions that the study group should address are the following:

- Which of the data being reported to TRs needs to be reported and stored in a sufficiently consistent and standardised form that it can be easily and accurately aggregated for financial stability monitoring and other purposes? It could also take into account the potential need in some cases for authorities in their financial stability analysis to combine aggregated OTC derivative data with data (gathered from other sources) on exchange-traded products or cash instruments.
- What types of data aggregates might authorities require for financial stability monitoring and other purposes (in light of the recommendations in the CPSS-IOSCO TR Access Report)?
- Does the data need to be reported in a globally consistent manner to TRs in the first place to make accurate global aggregation of the data feasible, or is it possible to develop a translation mechanism that will permit the aggregation of data originally provided in different formats? Are there any legal issues related to such translation? Do the answers to these questions differ between the different aggregation models?
- How can data standardisation best be achieved (for example by setting international standards for reporting of data to TRs, or by coordination between national authorities)?
- What are other elements that need to be standardized to achieve data aggregation such as business rules for producing the data content (e.g. data dictionaries); operational and technology standards for data normalisation/harmonisation, transfer, error handling and reconciliation?
- How can data be reconciled, so as to avoid double-counting and gaps in aggregated data? How might aggregation mechanisms address data quality problems that could undermine the usefulness of aggregated data?
- Should values be converted to a global currency to allow for cross-currency aggregation?

### III.2 Data access and associated legal issues for each aggregation model:

In considering the feasibility of each aggregation model, legal issues need to be considered, including the legal ability for data to be provided to the aggregating mechanism, as well as the legal ability of the aggregating mechanism to produce and share data with appropriate authorities. In considering these issues, the study group should draw upon the experiences and solutions found by other international data gathering exercises?

Among the questions that the study group should address are the following:

- What (if any) legal or procedural issues would there be in ensuring data can be sent from TRs into the aggregating mechanism? What requirements may this put on an aggregating mechanism to ensure data security is maintained? How do these legal issues differ between the different options for aggregating mechanisms?

- What legal and procedural issues would need to be addressed with regard to the production and sharing of aggregated data under each of the models? How might privacy and confidentiality issues and any other restrictions affecting authorities' access to TR data, such as indemnification requirements, affect the modalities for making aggregated data available under each of the options, either in terms of passing on aggregated data to a hub or providing the information to authorities?[6]
- Are these issues affected by whether the data are obtained by domestic or foreign authorities directly from TRs, from a hub, or via other authorities? How do those issues differ according to the scope of aggregation (for example, at a national or cross-border level or the form in which the data is being provided, e.g. anonymised or summarised)?
- Are there additional legal issues in cases where authorities may also require access the original data before aggregation, or may require access in a form that gives them flexibility to able to aggregate it in different ways (for instance by subsets of products or market participants)?
- What types of agreements could be needed to support each aggregation model? To what extent are data access and sharing needs covered by existing information sharing agreements, or are further agreements likely to be needed? How can questions of data security be dealt with?
- What are important preconditions in each jurisdiction related to data provision and use (e.g., multilateral or bilateral MoUs)? How would legal prohibitions, limitations, or preconditions affect the structure of the aggregation mechanism? How can such legal prohibitions, limitation, or preconditions be overcome via different operational solutions?
- Are there circumstances in which, for legal reasons, data may need to be aggregated first at a national level before cross-border aggregation takes place?

### III.3 Analysis of technical, organisational and operational issues of each aggregation model:

For each of the possible approaches to providing globally aggregated TR data to authorities, the study should examine the operational implications and issues, taking into consideration:

- existing TR infrastructure and data reporting standards;
- data privacy and confidentiality considerations, building on the work already conducted on these issues in the area of OTC derivatives and bearing in mind the different categories of data users amongst authorities;
- local languages and variations in existing national approaches to the representation of trades;
- the governance of the mechanism; including the relationship with overseers of TRs;

---

[6] Issues arising from current privacy and confidentiality restrictions on the reporting of data to TR and on the reporting of TR data to authorities are surveyed in the FSB's April 2013 OTC derivatives progress report. This feasibility study should consider any issues arising for the aggregation model from such restrictions.

– important practical aspects, such as time to implementation, technological requirements, operational reliability, adaptability and cost efficiency.

## IV. Composition of the feasibility study group

The feasibility study group is to be co-chaired by experts from member organisations of CPSS and IOSCO.

The composition of the study group is to be *ad hoc* including, in addition to experts from CPSS and IOSCO members, other experts from organisations not represented in these bodies that have roles in macroprudential and microprudential surveillance and supervision and the FSB Secretariat. The group should include a balanced representation of a range of expertise, covering aspects such as:

– data fields and formats;

– the potential needs of and uses by authorities of aggregated data;

– legal and regulatory considerations;

– IT and other technical issues.

At the same time, the number of members should be limited to approximately 20 people, to enable the study group to work expediently. The Secretariat for the study group will comprise members of the CPSS, FSB and IOSCO Secretariats.

The tight timeline and the potential interrelationships between data and legal issues imply that these two sets of issues should be explored in parallel. The study group should therefore set up two subgroups to consider respectively the technical data issues and the data access and legal issues. (This would be similar to the approach taken in the FSB's Data Gaps Implementation Group that is implementing a common data template for G-SIFIs.) These groups should coordinate closely in real time, through having some members in common, common secretariats and sharing of working papers, to ensure that interrelationships between the two sets of issues are taken account of. They should involve additional experts beyond the study group members as needed.

The study group may also set up other workstreams in specific areas as it sees fit, which may involve additional experts in specific areas.

## V. Schedule and deliverables

The group will need to work under an accelerated timeline, given the importance of rapid completion of the G20 reforms and effective use of TR data by authorities. The group should provide progress reports on the status of the work to the FSB, and for information to CPSS and IOSCO, including an interim report before end-September. The group should prepare a draft report by mid-January 2014 for review and approval by the FSB, with a view to requesting public feedback beginning no later than mid-February 2014.

The final report should be provided to the FSB no later than end-May 2014 and will subsequently be published. The FSB, in consultation with CPSS and IOSCO, will then make a decision on whether to initiate work to develop a global aggregation mechanism and, if so,

according to which type of aggregation model and which additional policy actions may be needed to address obstacles.

In taking forward the work, the group should engage with market participants and market infrastructure providers, having regard to geographical balance as well as with firms in the non-financial sector that have had successful experience in building functioning uniform global data infrastructure systems. As part of this engagement, the group should consider whether to host a workshop to discuss each aggregation model, its pros and cons and implementation approaches as part of its analysis.

# Appendix 2:
# Data Quality Dimensions

Data quality is deemed sufficient when the data are fit for purpose. In general, inaccuracies in underlying data are more acceptable when data are aggregated. When inaccuracies are small and the population is large, the data may still be considered 'fit for purpose' and may yield acceptable results when aggregated. The following dimensions of data quality apply from individual data elements in a trade report to highly aggregated summaries of transactions and positions and should be considered in the analysis of the data aggregation approaches:

***Completeness***

Missing or otherwise incomplete data for derivative products may lead to misleading conclusions. To ensure completeness of data for aggregation, the surest and most efficient way would have been for all TRs to collect and populate the same set of data elements. However, since such a unique TR data specification is not currently envisaged at an international level, a second best consists of ensuring that the data can be translated into a consistent standard. This still entails, though, significant constraints regarding specifications of the data stored by TRs.

***Accuracy***

The values for a data element must conform to a standard definition and meaning to be accurate. Likewise, the data elements collected by each TR should have unambiguous shared meaning and conform to standards for their content values in order for data aggregated across TRs to be accurate. Deviations from a standard definition and meaning for a data element might result in the uneven acceptance of valid values across TRs, degrading the quality of the data.

***Timeliness***

In order to be timely, data must be available when and where needed, and provide the most current content. However, aggregation across TRs is challenged by the collection mandates and reporting calendars of authorities globally. This includes any differences in the requirements for the frequency and location of data access by authorities and the frequency and location for data collection from market participants.

Since OTC derivatives contracts are often active over long periods of time the standards for maintaining and refreshing data have to be determined and harmonised across TRs and jurisdictions. Depending on the chosen scenario, the responsibility for updating data should be clarified, whether relying on TRs or on the global aggregation mechanism since this could hinder consistent aggregation.

***Consistency***

Data must have unambiguous shared meaning, allowable values, and business rules for their creation, maintenance, and retirement among the TRs. Without consistency, the quality of data across TRs will vary and negatively affect the ability to rely on the results of aggregation

of transactions and positions. The agreement and setting of standards for TR data is a necessary condition to achieve consistency.

***Accessibility***

To be accessible, collected data must be available to authorities where and when needed. Accessibility for aggregation is dependent on both the technological capability (including the data security systems and controls that govern permission to access data and the agreement among authorities on the TR governance process) and the legal agreement that grants authorities access to the data.

Quality

***Duplication***

This dimension, often referred to as 'Uniqueness', is critically important to the prevention of double-counting of transactions and positions across TRs. The development of standards for unique entity, instrument, and transaction identifiers provides the foundation for the prevention of duplication. As described in Chapter 3, avoidance of duplication is necessary for the purpose of aggregation. Standards for data content are in turn necessary to provide the capability to identify, correct, and prevent data duplication both within and among TRs.

***Integrity***

Data integrity involves ensuring that the processing involved in the aggregation does not distort or misrepresent the data that were originally reported.

**Operational factors contributing to high quality TR data**

Data quality must be addressed from the moment the data is reported to the TR and at every point where data are exchanged. Both technical and business data quality practices must be applied to ensure the interoperability of the data among market participants, TRs and authorities.

The following operational aspects of data quality may need to be considered to facilitate proper data aggregation:

- Whether the data are technically capable of being processed by the receiver and contain meaningful values.
- Whether validation can be performed on the data to ensure consistency and completeness, and to avoid duplication.
- Whether there are further checks for accuracy that could or should be carried out seeking to ensure that the reported items are correct.
- Whether data quality is being managed proactively or reactively.
- Whether and what combination of technical and business data quality checks are undertaken.

While individual TRs will carry out validation of the data that is reported to them it is important that various TRs operationalise data quality processes in a consistent way[1]. Thus the discussion here is about the data quality issues that are pertinent to integration of data from several TRs for aggregation rather than data quality from the point of view of a single TR.

A variety of technical checks would need to be conducted including checks for conformance to standards, format, allowable values, and internal consistency. Such checks would require some sort of a data dictionary and validation rules that define the allowable formats and values of the individual items or groups of items. This implies that an agreed-upon set of definitions and meanings of the data by industry participants, TRs and authorities is essential, regardless of the aggregation mechanism. Some of these checks would also require access to reference data, such as those for counterparty and product identifiers as well as elements like country and state codes, including having a robust reference data management function.

[1] It is assumed that ensuring that the reports submitted to the trade repositories meet quality standards is outside the scope of any central aggregation solution. This role will be performed variously by the trade repositories themselves and the supervisors of the trade repositories and reporting entities according to the rules prevailing in a specific jurisdiction.

# Appendix 3:
# Extract from Table 6.2 of the Access Report

| | **Assessing systemic risk (examining size, concentration, interconnectedness, structure)** | **Evaluating derivatives for mandatory clearing determinations and monitoring compliance with such determinations** | **Evaluating derivatives for mandatory trading determinations and monitoring compliance with such determinations** | **General macro assessment** | **Conducting market surveillance and enforcement** |
|---|---|---|---|---|---|
| Definition | An authority with a mandate to monitor a financial system and to identify emerging risks | An authority that has a mandate to evaluate OTCD for mandatory clearing determinations and monitoring its implementation | An authority that has a mandate to evaluate OTCD for mandatory trading determinations and monitoring its implementation | An entity that has a mandate to foster and support financial stability globally | An authority that has a mandate to conduct market surveillance and enforcement |
| Typical depth of data required | Transaction-level | Transaction-level | Transaction-level | Position-level | Transaction-level |
| Typical breadth of data required | All counterparties | (1) Any transactions in which one of the counterparties is within its legal jurisdiction and (2) all transactions on the underliers (i) within its legal jurisdiction (whether the counterparties are in the jurisdiction or not), (ii) for which the authority considers making or makes a mandatory clearing determination, or (iii) any transactions involving the same type of OTCD contract as the one being evaluated (whether the counterparties or underliers are in the jurisdiction or not) | (1) Any transactions in which one of the counterparties is within its legal jurisdiction and all (2) transactions on the underliers (i) within its legal jurisdiction (whether the counterparties are in the jurisdiction or not) or (ii) for which the authority must make a mandatory trading determination | All counterparties | Any transactions for counterparties in its legal jurisdiction as well as branches or subsidiaries of these counterparties which may be in other jurisdictions, and all transactions on the underliers within its legal jurisdiction (whether the counterparties are in the jurisdiction or not) |
| Identity | Named data for counterparties and underliers within their legal jurisdiction. Anonymised data for other counterparties | Anonymised counterparties and named data where named data are required for evaluating determinations; named data for monitoring compliance with such determinations | Anonymised counterparties and named data where named data are required for evaluating determinations; named data for monitoring compliance with such determinations | Anonymised | Named data |

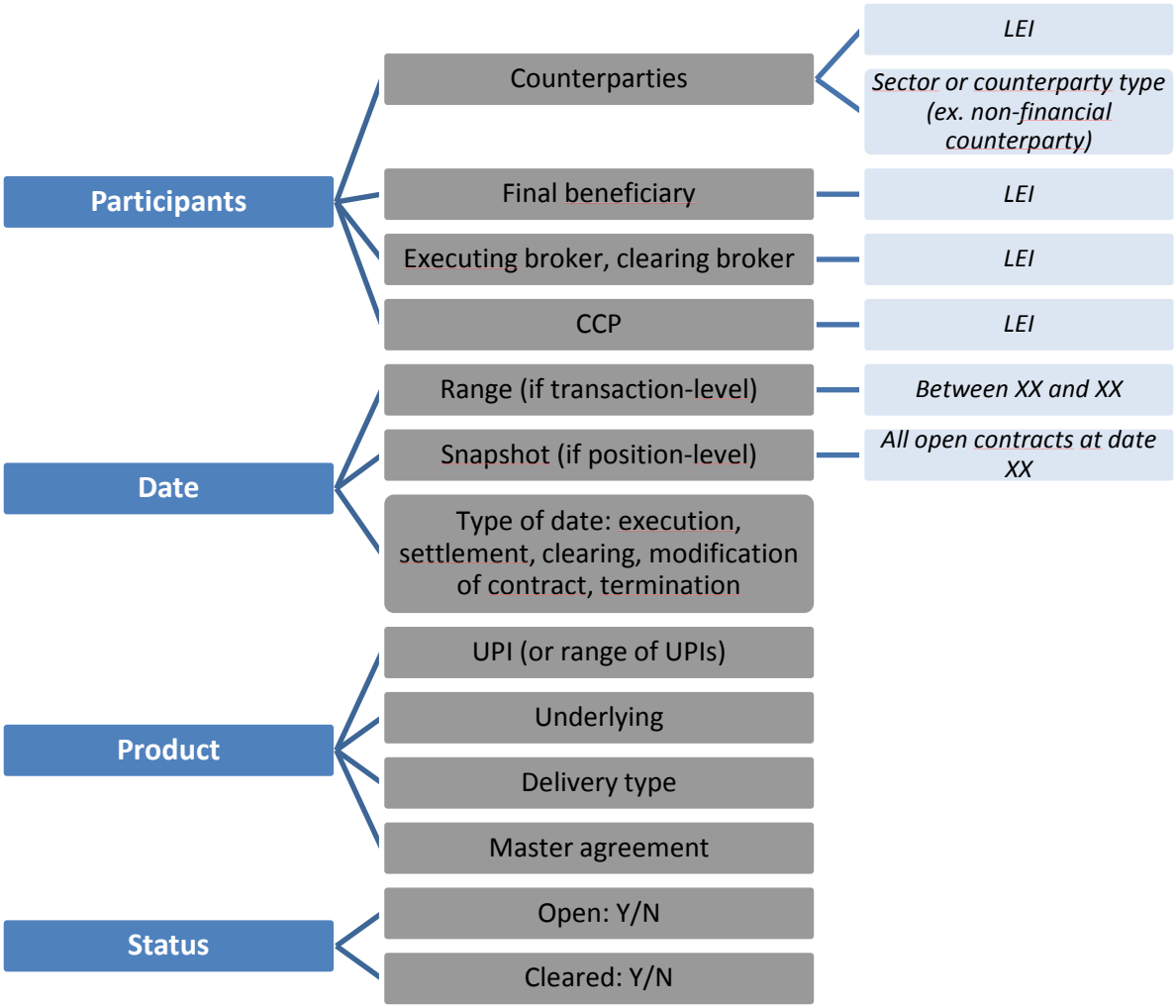
| | **Registering and regulating market participants and supervising market participants with respect to business conduct and compliance with regulatory requirements** | **Prudentially supervising financial institutions** | **Supervising/ overseeing exchanges, organised markets and organised trading platforms** | **Regulating, overseeing and supervising payment or settlement systems** | **Regulating, overseeing and supervising CCPs** | **Regulating, overseeing and supervising TRs** |
|---|---|---|---|---|---|---|
| Definition | An authority that has a mandate to supervise market participants. | An authority that has a mandate to supervise and regulate or to monitor and conduct surveillance on the financial institution | An authority that has a mandate to supervise exchanges, organised markets and organised trading platforms | An authority that has a mandate to oversee a payment or a settlement system | An authority that has a mandate to supervise or oversee a CCP | An authority that has a mandate to supervise a TR |
| Typical depth of data required | Transaction-level | Transaction-level | Transaction-level | Transaction-level | Transaction-level | Transaction-level |
| Typical breadth of data required | Transactions in which one of the counterparties, whether registered or not, is within its legal jurisdiction, or in which one of the counterparties engages in OTCD transactions with, or whose OTCD transactions are guaranteed by, an entity within its legal jurisdiction (whether the counterparties are in the jurisdiction or not) | Transactions in which one of the counterparties is a consolidated organisation whose parent is supervised by the authority, including all subsidiaries, domestic or foreign, of the entity | Any transactions traded on an exchange, organised market or organised trading platform supervised by the authority | Any transactions settled by a payment or settlement system overseen by the authority | Any transactions that are cleared by a CCP supervised or overseen by the authority | Any transactions reported to the TR |
| Identity | Named data | Named data | Named data | Anonymised transaction-level data as a general rule, but named position-level data for the counterparties of the central bank and where investigation of suspicious activity is needed. | Named data | Named data |

| | Planning and conducting resolution activities | Managing currency policy | Implementing monetary policy | Lender of last resort function |
|---|---|---|---|---|
| Definition | An authority that has a mandate to resolve financial institutions | An authority in its function as monetary policy authority | An authority in its function to implement monetary policy | An authority in its function as possible lender of last resort |
| Typical depth of data required | Transaction-level | Transaction-level (Participants within legal jurisdiction), aggregate-level (all participants for underliers denominated in its currency) | Aggregate-level | Position-level |
| Typical breadth of data required | Any transactions in which one of the counterparties is the entity subject to resolution or a domestic or foreign affiliate | Any transactions that specify settlement in that currency, including transactions for which that currency is one of two or more specified settlement currencies | Any transactions for participants within a central bank's legal jurisdiction or underliers denominated in a currency for which the central bank is the issuer | Any transactions for which a named institution is a counterparty |
| Identity | Named data | Anonymised | Anonymised | Named data |

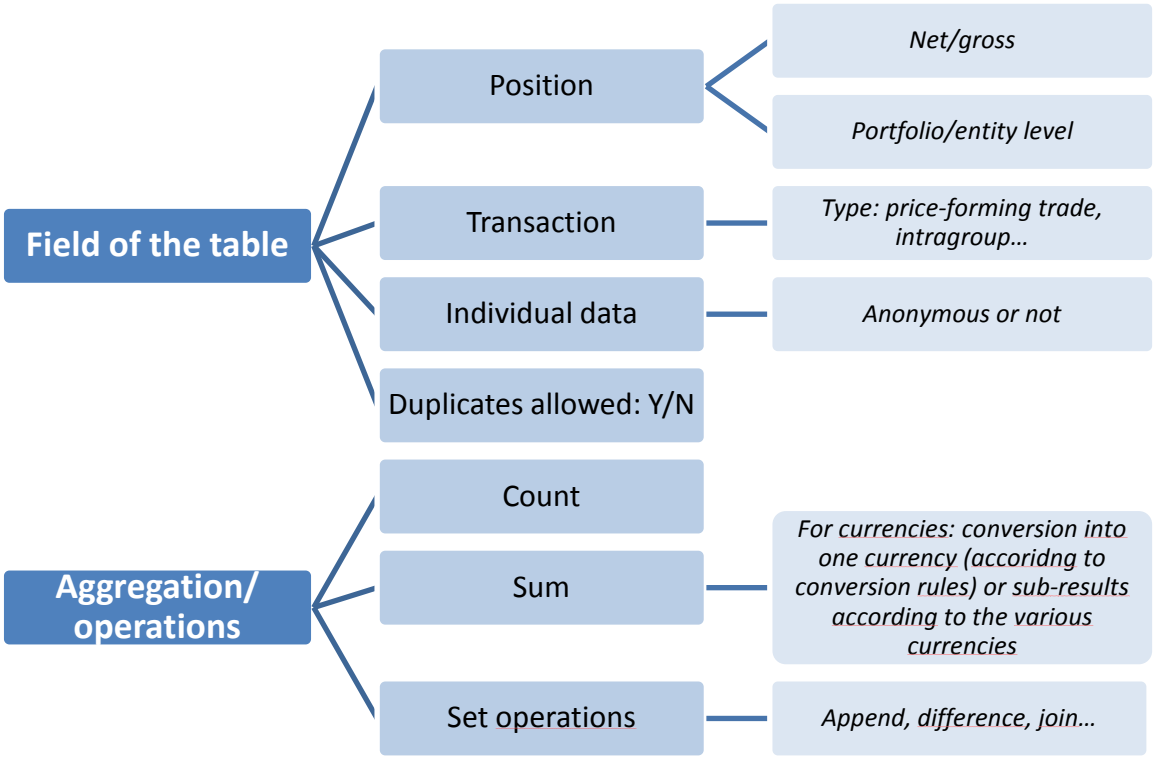
# Appendix 4:
# Data Elements

Data elements needed to perform queries for various regulatory purposes can be classified in various ways. The list of data fields depends on the mandate of the user and shall be adapted according to the specification and particular type of the aggregation system. The diagram below shows different examples of data elements that may be used by users to perform a request.

Another list of fields data elements (below) is intended to allow the user to describe the form of the result expected This includes the specification of expected data elements and of operations to be performed on the data, such as summing or counting. Depending on their mandate, some users will have limited ability to define the form of the result, for instance some of them might be obliged to perform summation over specific data elements.




From the standpoint of a user, the requests and the results need to be independent from the specific implementation of the system. The different requests described here could be performed under any of the options discussed in this report.


Field of the table
Position
Net/gross
Portfolio/entity level
Transaction
Type: price-forming trade, intragroup…
Individual data
Anonymous or not
Duplicates allowed: Y/N
Aggregation/ operations
Count
Sum
For currencies: conversion into one currency (accoridng to conversion rules) or sub-results according to the various currencies
Set operations
Append, difference, join…

# Appendix 5:
# Summary of the outreach workshop

**FSB Aggregation Feasibility Study Group (AFSG) outreach workshop**
**Summary of the meeting in Basel, 13 November 2013**

The FSB AFSG Industry Workshop was conducted in Basel, Switzerland on November 13, 2013. The purpose of the workshop was for the AFSG membership to understand industry perspectives, approaches and practices to aggregation and apply those to the development and assessment of the different options for Trade Repositories (TR) aggregation being considered by the group following the FSB mandate.

## I. Opening remarks

The co-chairs of the FSB feasibility study group on approaches to aggregate OTC derivatives data, Mr Benoît Cœuré (ECB) and Mr John Rogers (US CFTC) welcomed the outreach workshop participants. They noted that the purpose of the event was to learn about various options of the data aggregation from different aspects. The specific objective of the workshop was to assist the group in its work to identify the pros and cons of mentioned three options for aggregation:

1. A physically centralised model of aggregation.
2. A logically centralised model of aggregation based on federated (physically decentralised) data collection and storage.
3. Collection of raw data from local TR databases by individual authorities that then aggregate the information themselves within their own systems.

The co-chairs indicated that the workshop would address both technical and legal issues in relation to the implementation of the alternative options, and the AFSG had invited attendance of experts with expertise in the range of issues involved, including data, IT and legal issues.

## II. Panels to discuss current approaches to data aggregation (inside and outside the financial sector)

### A. A physically centralised model of aggregation

*Panellists: Trade Repository Limited, LSE, SAMA-TR*

The panel on physically centralised model of aggregation focused on how the model would be defined, what the pros and cons are and what the potential hurdles for implementation are and how to overcome them. The panellists presented their experiences and advise on the aspects to consider in developing and assessing such a model.

The current data aggregation challenge was presented where aggregated number of reports is not equal to the market's exposure. That creates an issue of how the data aggregated from TRs actually allows regulators to meet various regulatory needs. The objectives of instrument/product data were enumerated in order to achieve regulatory data use: global scale, multiple purpose, automated analysis, automated aggregation, cross market focus. The participants suggested that a semantic representation using a concatenation of standardised building blocks can be helpful to overcome the global data aggregation challenge. It was noted that with source data (i.e. data that can be aggregated) and timely additive partial composites, the meaningful observations of changes to market flows and exposures are readily available just days after trades are done and that even with limited coverage this enables better market oversight and systemic risk analysis and management.

Participants also stated that before going into selection of aggregation models the following questions need to be answered: Are all the current derivative reporting regulations compatible? How do you ensure data is not duplicated? How is access to data governed and approved? What can be done to ensure the consistency of the data? What is being aggregated? Participants emphasised that governance is one of key dimensions of a physically centralised model.

It was also mentioned that when implementing a physically centralised model on the local level, the unavailability of standardised taxonomies for the contracts was a challenge. Consequently, the TRs had to develop standards and shared them among reporting entities. That facilitated the ability to aggregate and compare the reported data. Participants also explained their experiences in implementing and developing standards that would assist in the harmonisation and description of complex OTC derivatives data which would in turn assist aggregation efforts.

The participants also explained their experiences and challenges in implementing the model under different circumstances including management of stakeholders, technical planning, project planning, access governance, project management as well as technical implementation.

## B. A logically centralised model of aggregation based on federated approach

*Panellists: ANNA, GS1, Quartet FS, DTCC, Denodo*

The session focused on the logically centralised model of aggregation based on a federated data collection and storage. The objective was to answer the following questions: What is the logically centralised model? How can it be implemented? What are the obstacles and how can they be overcome? Participants made it clear that several variants might exist under the logically centralised model label. While such model is in essence characterised by the combination of data remaining stored in local repositories and the existence of an index, the scope of the data contained in that index may vary widely. On one extreme the index may be populated with only a list of identifiers with pointers to the local repositories. In such a scenario, the index would not store actual data but only references. However, when the data get complex - and also depending on the complexity of the queries - the index would have to store (cache) some data for the mechanism to produce the expected outcome. In any case, it is a key that the index can be trusted and is thus properly governed. As an overall consequence, participants considered that a logically centralised model can mitigate some legal issues

compared with a centralised model when processed data are confidential, but the extent to which it could achieve this would ultimately depend on the data held in the index and the nature and of oversight/supervision or governance of the index operator.

In the context of financial transactions, participants considered whether it was likely that the aggregation mechanism would require more data held in some version of a centralised unit in order to perform indexing. In this respect, participants underscored that the nature of the data processed - whether public as in the LEI framework or private and confidential as data held in TRs - would be a key matter to bear in mind.

Some participants opined that the logically centralised model might not be the most efficient one for complex queries. They also highlighted the need to make the aggregation mechanism flexible and scalable. For example, participants made clear that the mechanism should be flexible regarding the incorporation of new queries and further (new established) TRs. Some participants stated that they would not recommend pre-aggregation of data and advised that the aggregation mechanism should use the raw transactional data to produce the aggregated outcome of good quality.

More generally, and beyond the issue of the model to be adopted, participants noted that a clear identification of the objective of the aggregation with a distinction between local regulatory objectives and global ones would help to identify the granularity of the data needed as well as governance model. However, they admitted that the use of raw data raises a number of the issues on confidentiality and volume/cost issues that should not be ignored. In addition, they opined that the use of raw data may also increase the expectations on the role of the index and its operator, or at least of the rules that entities using the index should follow (to ensure harmonised aggregation).

Some participants highlighted that the distinction between the content of the data to be captured and the move of the data among the interested parties (”choreography”) is an important feature of a logically centralised model. In order for the model to work and to provide good-quality data, the participants felt that content has to be clearly defined and be the same among the actors of the model regardless of the choreography, while choreography might vary based on circumstances. In contrast, there might be different styles of choreography (where the data reside, when and how they move between partners, regulators, repositories) with a need to be able to change the choreography to match varying processes. Regarding the content, and in the context of financial transactions, participants observed that product scope varies by jurisdictions, including the definition of derivative contracts. Therefore, they expressed that there is a need for regulators to look at open sources and standards supported by industry stakeholders - and to promote globally recognised identifiers wherever possible.

Participants felt that adequate procedures (criteria for membership, regular (standardised) report) need to be in place to generate trust.

Finally, participants mentioned several additional benefits of the logically centralised model, in terms of scalability, tailoring to local needs and cost reduction through competition, but also warned that many initiatives have failed due to costs.

## C. Data collection and aggregation by users from local sources

*Panellists: ACTUS, NSD, ICE, Bloomberg, NOAATS, CME Group*

Panellists presented their views on data collection and aggregation by users from local sources and potentially at local level. It was noted that the objective of aggregation is to get meaningful financial analytical information. Simple aggregation of disparate financial instruments does not support this objective because there is no common metric to support such aggregation. It is akin to trying to add apples and oranges. Meaningful financial analytical information is derived from the ability to understand how changes in risk factors affect value, income, liquidity, and stress tests. Such analyses start with the ability to represent how changes in risk factors affect the cash flows associated with individual financial contracts. The example of algorithmic contract types unified standards (ACTUS) was introduced to solve this problem. It is being developed to generate the common metric of state contingent cash flows for all financial contracts. Such state contingent cash flows are the starting point for a broad range of financial analyses. These analysis results can then be aggregated for any size pool of financial obligations -- portfolios, single institutions, individual markets, or the financial system -- to yield meaningful financial analytical information.

Participants expressed the view that the following core principles for the TRs needed to be introduced to guide the feasibility analysis: (a) transparent and high standards governance; (b) minimal operational processing; and, (c) adherence to current and future rules of regulatory authorities. That would require common data on counterparties; products, trades, venue(s) of execution, price, quantity, Central Counterparties (CCPs) at minimum. For the purpose of data aggregation the TRs face a number of challenges that need to be addressed such as collection of accurate data, clarity on fields being reported to TRs; data harmonisation where there is a lack of consistency among TRs on the interpretation of data requirements. Data security was emphasised as a key consideration.

Participants also described the common ETL (extract/transform/load) approach that could be applied for data aggregation: (a) extraction of external data from sources; (b) transformation/conversion of external data into internal target format where data needs to be normalised so it can be aggregated and accurate meaning can be inferred from it; and, (c) finally load of useable data to target database. Different depths of access were introduced for different data types to achieve aggregation purposes. Participants noted that local/federated type data aggregation might work. Data sharing between authorities could be done using standard framework under reciprocal agreement – however legal issues would need to be addressed in terms of what can be shared across jurisdictions. Different views were presented on what model is more expensive for implementation and long-run maintenance.

Panellists emphasised that while legal and technical issues on collecting transaction level data by each local TR could be addressed with relatively less effort, global collection and aggregation of OTC derivatives data could raise many issues between countries and various stakeholders within each country depending on the access level. As a practical way forward, equal accessibility by every country to the data was suggested. In this context accessibility means literal ability to access global data and capability of an authority to achieve its goal by using the data. The participants felt that UPI system standard was vital for data aggregation.

## III. Data considerations

*Panellists: FIBO, FIX, FpML, ISO*

The panel on Data Consideration discussed matters related to data and data standards and how to leverage them for aggregation. Participants noted a number of times that data standardisation was a key tool for data aggregation. They also noted that the focus should be on standardisation of content rather than on formats. Participants noted that the biggest standards gap is in the area of financial language and unambiguous shared meaning (definitions). They also noted that existing standards used by (participants/TRs/regulators) can be leveraged if mapped to a common meaning.

Panellists also elaborated on the difference between semantics and syntax of standards. They noted that terminology plays a major role in understanding semantics and that a common terminology with definitions and 'translations' would be helpful here. They further noted that without standards for counterparties, instruments and trades, it would be hard to make quick progress in data aggregation. Counterparties and instruments might be subject to a hierarchical structure and relationships between entities may be of interest when aggregating data. Participants stated that reporting of aggregated data requires an upfront and detailed specification, and noted that if such a specification is ambiguous, it might result in a lack of harmonisation and, worse, in misaggregation and thus unreliable data. Participants stated that reporting of transaction level data is easier as it is primarily about passing through data from market participants yet they noted that it raises more confidentiality and thus governance issues.

Participants also introduced their ideas about structure of UTIs and UPIs. In particular, they noted that UTI generation and communication should occur at earliest possible point in trade flow. One of the suggestions was to use a prefix in UTI construct focused on utilizing the CFTC USI namespace in the construction of the UTIs. With respect of to the UPI, one of the suggestions was to use ISDA OTC taxonomy. Under this model, they noted that the ISDA Asset Class Implementation Groups and Steering Committees proposed and approved this governance structure. It was also suggested that no country- specific IDs should be used and that only global codes, such as the LEI, should be used. It was also noted that there is a need for collaboration between regulators and endorsement by regulators of the development of a unique global trade and product identifiers. Otherwise, we risk having multiple identifiers, which defeat part of the purpose and will make the work of aggregation more difficult.

Furthermore, participants suggested that existing identification and classification schemes should be used as far as possible. They noted the experience of common data dictionaries under ISO 20022 (ISO 20022 "Investment Roadmap" integrated FIX, FpML, ISO (MT/MX) and XBRL into a common framework). It was also noted that only open- access and non-proprietary standards should be used in order to avoid competition issues and not to discriminate against smaller operators.

# IV. A. Legal considerations in data aggregation

*Panellists: ISDA, STET, DTCC, BM&FBOVESPA*

The session focused on the potential legal issues that might arise from the data aggregation framework. Firstly, participants pointed out existing legal issues such as privacy and confidentiality, intellectual property, indemnification, and data access. An example of the centralised hub for derivatives introduced in Brazil (due to their 3 TRs) was presented to participants. The Brazilian system also includes valuation data and the registration in a TR is a condition for legal validity of the contracts.

With regard to data aggregation schemes, participants asked for more clarity on which authorities have access to what kinds of data and for what mandate. In order for authorities to share the data, while ensuring the data security/protection, participants suggested that authorities might want to consider establishing a framework of multilateral MOU, possibly leveraging MoUs such as IOSCO Multilateral MOU.

Though participants noted that anonymisation could help to solve the confidentiality issue, they questioned how authorities could aggregate and properly use such data for assessing and monitoring systemic risk and monitoring financial markets in general without names or unique identifiers. Also they noted that the method of anonymisation needs to be consistent amongst TRs. One of the proposals was to establish a harmonised model to regulators as they bear a general duty to keep data confidential while ensuring regulators get access to the data appropriate to their mandates. This could also be extended to the public, in aggregate form (data dissemination duty). Some participants felt that legal issues might be less complicated if the data could be aggregated and then distributed to authorities than a case where providing authorities are provided with direct access to detailed data however others disagreed with the position. Participants also noted that different jurisdictions have different requirements for OTC derivatives reporting (e.g. US position reporting versus EU reporting of contracts, the latter putting the responsibility to calculate positions on the TRs themselves).

Some participants noted that the data level of detailed data depends on the purpose of data collection and suggested that if the purpose of data aggregation is to have general view of the OTC derivatives markets, classification such as banks, hedge funds, pension funds etc. might suffice to support such an objective.

Regarding individual clients (natural persons), participants pointed out that reporting requirements vary from country to country. They noted, for example that, in Japan, in a case where counterparty is not a bank, it is not necessary to report specific names but only classification as ‘client’.

The participants argued that, given the large volumes of data, it might be enough to collect and analyse the data of relatively large reporting firms (e.g., top-ten firms and top-ten counterparties). They opined that if authorities observed any potential risk, then the relevant national authorities could have access to the raw data to analyse at a deeper level. In that sense, collecting data from large entities would possibly satisfy the need/objective to analyse the systemic risk.

Participants noted that generally there exists no legal intellectual property (IP) rights on raw data but data aggregated by TRs could be protected pursuant to the relevant IP rules and laws.

The term 'ownership' was discussed regarding data access rights. One commenter suggested that TRs only have the rights to use the data as described by regulations the legal and contractual rules under which they operate. This is an important factor on disclosure of data as TRs do not own the data they received and are bound by a legal obligation of confidentiality towards their clients by its participants and under regulation.

Participants recalled that authorities have access to the data held at TRs in their jurisdictions, for their specific mandates. In addition, in the cross-border context, authorities have access to the data to fulfil their mandates based on the CPSS-IOSCO Access Report. In these cases, confidentiality is still an issue since the data needs to be kept secure (in authorities' domain).

## IV. B. Technology considerations

*Panellists: Denodo, PRMIA, Sapient, TriOptima*

In this section participants focused on technology considerations for analysis of data aggregation models. Among technical dimensions, data standards, aggregation methodology and system architecture were outlined. On the business and policy dimensions participants discussed commercial incentives, practical reality and political will as well as trust. Participants also noted the overlapping dimension of the access choreography that needs to be carefully structured. The docking model of financial data compression was introduced where the transaction aggregation systems provide access via extraction, transformation and load to granular data that is being aggregated via tuneable, multi-dimensional processor.

Participants introduced the idea of service centres which harvest and manage data from various repositories. It was noted that the challenge of complex structured deals would be addressed by the opportunity of visual data navigation tools. Participants emphasised that data size is not a real issue but data standardisation, cost and complexity are the issues to focus on. Participants introduced data virtualisation. This approach decouples data complexities from the business logic; defines canonical data models for business units; utilises central governance for security and data lineage, provides data on demand either via cache or scheduled batch; allows reuse of models which are easy to transform, combine and change data, reduces replication costs; and integrates with existing tools.

Participants also discussed the concept of exposure and repository reconciliation. They identified five important targets when discussing technical considerations and conceptual architecture: scalability, availability, confidentiality, integrity and sustainability.

Participants made a distinction between two data aggregation models from the standpoint of anticipated analysis - reactive approach versus a proactive approach. In reactive approach analysis is undertaken when triggers locally require an extended scope of analysis. Participants felt that from this standpoint it reduces resilience requirements as system up-times are required for retrospective forensic analyses rather than real time monitoring. Participants discussed whether repositories' primary purpose is for storage and forensic analysis. Participants stated that for valuable forensic analysis, a complete non-aggregated record is preferred with low data sharing restrictions. On the other hand, proactive approach provides for configured analytics trending on data to highlight potential risks. Here resilience requirements are increased as analytical success is dependent on robust data delivery. Participants stated that in this case, the primary purpose is to highlight trends of concern.

Participants noted that at the same time data sharing and aggregation can be restricted to satisfy extra territorial restrictions and harmonised canned reports required to push trend and analytics data to regulators.

## V. Summary of takeaways from subgroup discussions and closing remarks

The co-chairs thanked the workshop participants for their insights and professional opinions which would be a useful basis for the FSB group AFSG analysis. They encouraged participants to provide further comments on the consultative report of the group to be released in February 2014 as a continued engagement in the public-private consultation process.

**List of private sector participants for the FSB outreach workshop on approaches to aggregate OTC derivatives**

**Basel 13 November 2013**

| | |
|---|---|
| **Bloomberg L.P.** | **Ravi Sawhney**<br>Head of Fixed Income Credit Trading |
| **BM&FBOVESPA** | **Marcelo Wilk**<br>OTC Operations Officer |
| **The Central Securities Depository of Poland (KDPW S.A.)** | **Leszek Kolakowski**<br>Vice Director, Strategy and Business Development Department |
| | **Kinga Pelka**<br>Specialist, Trade Repository Department |
| **CME Group** | **Jonathan Thursby**<br>President, CME Swap Data Repository |
| **Denodo Technologies** | **Gary Baverstock**<br>Regional Director, Northern Europe |
| **FIX - Deutsche Börse AG** | **Hanno Klein**<br>Senior Vice President |
| **DTCC** | **Marisol Collazo**<br>DerivSERV |
| **FIBO - EDM Council, Inc** | **Michael Atkin**<br>Managing Director |
| **Fincore Ltd** | **Soeren Christensen**<br>CEO |
| **George Washington University Law School** | **Navin Beekarry**<br>Researcher, Lecturer |
| **GS1** | **Kenneth Traub**<br>Standards Strategy Consultant |
| **Intercontinental Exchange** | **Kanan Barot**<br>Director, Ice Trade Vault Europe |
| **ISO – Investment Management Association** | **David Broadway**<br>Senior Technical Adviser |

| | |
|---|---|
| **ISDA** | **Karel Engelen**<br>Director, Global Head Technology Solutions |
| **ISDA – Deutsche Bank** | **Stuart McClymont**<br>ISDA data and reporting steering committee |
| **KOSCOM** | **He Young Jun**<br>Assistant Manager, Global Business Department |
| | **Gi Young Song**<br>Assistant Manager, System Department |
| **LCH.Clearnet. Ltd** | **Richard Pearce**<br>Business Change Manager, SwapClear |
| **London Stock Exchange Group (LSEG)** | **James Crow**<br>Head of Product Solutions & Development |
| | **Neil Jones**<br>Product Solutions Architect |
| **ANNA - Malta Stock Exchange** | **Stephanie Galea**<br>Senior Manager, Compliance & Market Operations |
| **Mizuho Bank Ltd** | **Satoru Imabayashi**<br>SVP and Head of Planning, Market Coordination Div. |
| **National Settlement Depository** | **Pavel Solovyev**<br>Head of Trade Repository Development |
| **NOA ATS** | **Kibong Moon**<br>CEO |
| **Nomura** | **Kieron O'Rourke**<br>Global Head of OTC Services |
| **Project ACTUS** | **Allan Mendelowitz**<br>Strategic Adviser |
| **QUARTET FS** | **Catherine Peyrot**<br>Senior Sales Executive |
| | **David Cassonnet**<br>Program Director |
| **REGIS-TR** | **Mari-Carmen Mochon**<br>Project Manager |

| | |
|---|---|
| **RTS** | **Alexandra Kotelnikova**<br>Chief Expert, Regulatory Support Department |
| **Sapient Global Markets** | **Cian O'Braonain**<br>Regulatory Reporting Practice Global Lead |
| | **Peter Newton**<br>Senior Manager, Markets Infrastructure Initiatives |
| **Saudi Arabian Monetary Agency** | **Abdulaziz Alsenan**<br>Project Manager, General Department of Payment Systems |
| | **Mohammed Al Hossaini**<br>General Department of Payment Systems |
| **STET** | **Fabienne Pirotte**<br>Legal Counsel |
| **Sumitomo Mitsui Banking Corporation** | **Kenji Aono**<br>Deputy General Manager, Corporate Risk Management Dept |
| **SWIFT** | **Yves Bontemps**<br>Head of Standards R&D |
| **PRMIA - Tahoe Blue** | **Jefferson Braswell**<br>CEO, Founding Partner |
| **The Trade Repository Ltd** | **Marcelle Kress von Wendland**<br>CEO |
| **Traiana Ltd** | **Mark Holmes**<br>Programme Manager |
| **TriOptima** | **Henrik Nilsson**<br>Head of Business Development |

# Appendix 6:
# Aggregation Feasibility Study Group participants

| | |
|---|---|
| **Co-chairs:** | **Benoît Coeuré**<br>European Central Bank |
| | **John Rogers**<br>US Commodity Futures Trading Commission |
| **Vice-chairs:** | **Simonetta Rosati (until November 2013)**<br>**Karine Themejian (from November 2013)**<br>European Central Bank |
| | **Srinivas Bangarbale**<br>US Commodity Futures Trading Commission |
| **Australia** | **Jennifer Dolphin**<br>Australian Securities and Investment Commission |
| **Brazil** | **Sergio Ricardo Silva Schreiner**<br>Securities and Exchange Commission |
| **Canada** | **Joshua Slive**<br>Bank of Canada |
| | **Andre Usche**<br>Bank of Canada |
| | **Shaun Olson**<br>Ontario Securities Commission |
| | **Jean-Philip Villeneuve**<br>Québec AMF |
| **China** | **Shujing Li**<br>China Securities Regulatory Commission |
| | **Zhu Pei**<br>China Securities Regulatory Commission |

| | |
|---|---|
| **France** | **Priscille Schmitz**<br>Banque de France |
| | **Olivier Jaudoin**<br>Banque de France |
| | **Yann Marin**<br>Banque de France |
| | **Sébastien Massart**<br>Autorité des Marchés Financiers |
| **Germany** | **Sören Friedrich**<br>Deutsche Bundesbank |
| **Hong Kong** | **Colin Pou**<br>Hong Kong Monetary Authority |
| | **Pansy Pang**<br>Hong Kong Monetary Authority |
| **India** | **Sudarsana Sahoo**<br>Reserve Bank of India |
| **Italy** | **Carlo Bertucci**<br>Banca d'Italia |
| **Japan** | **Osamu Yoshida**<br>Financial Services Agency |
| | **Hiroyasu Horimoto**<br>Financial Services Agency |
| | **Shoji Furukawa**<br>Financial Services Agency |
| **Korea** | **Namjin Ma**<br>Bank of Korea |
| | **Jerome(Jae Hyuk) Shin**<br>Bank of Korea |
| **Netherlands** | **Rien Jeuken**<br>De Nederlandsche Bank |
| **Russia** | **Philipp Ponin**<br>Central Bank of the Russian Federation |

| | |
|---|---|
| **Saudi Arabia** | **Abdulmalik Al-Sheikh**<br>Saudi Arabian Monetary Agency |
| **South Africa** | **Marcel de Vries**<br>South African Reserve Bank |
| **Sweden** | **Loredana Sinko**<br>Sveriges riksbank |
| | **Malin Alpen**<br>Sveriges riksbank |
| **Switzerland** | **Patrick Winistoerfer**<br>Financial Market Supervisory Authority |
| **UK** | **Nick Vause**<br>Bank of England |
| | **John Tanner**<br>Financial Conduct Authority |
| **US** | **James Corley**<br>Commodity Futures Trading Commission |
| | **Cornelius Crowley**<br>Department of the Treasury |
| | **Angela O'Connor**<br>Federal Reserve Bank of New York |
| | **Kathryn Chen**<br>Federal Reserve Bank of New York |
| | **Janine Tramontana**<br>Federal Reserve Bank of New York |
| | **Celso Brunetti**<br>Federal Reserve Board |
| **European Commission** | **Muriel Jakubowicz**<br>**Julien Jardelot** |
| **European Securities and Markets Authority** | **Frederico Alcantara** |
| **International Organization of Securities Commissions (IOSCO)** | **Tajinder Singh**<br>**Yukako Fujioka** |

| | |
|---|---|
| **Committee on Payment and Settlement Systems (CPSS)** | **Klaus Martin Löber**<br>**Philippe Troussard** |
| **FSB Secretariat** | **Rupert Thorne**<br>**Irina Leonova**<br>**Uzma Wahhab** |

# Appendix 7:
# Abbreviations

| | |
|---|---|
| **Access Report** | August 2013 CPSS-IOSCO report on authorities' access to TR data. |
| **AFSG** | Aggregation Feasibility Study Group |
| **BCM** | Business Continuity Management |
| **BIS** | Bank for International Settlements |
| **CCP** | Central Counterparty |
| **CDS** | Credit Default Swap |
| **CFTC** | US Commodity Futures Trading Commission |
| **CPSS** | Committee on Payment and Settlement Systems |
| **Data Report** | January 2012 CPSS-IOSCO report on OTC derivatives data reporting and aggregation requirements. |
| **EMIR** | European Market Infrastructure |
| **ESMA** | European Securities and Market Authority |
| **EU** | European Union |
| **FMIs** | Financial Market Infrastructures |
| **FSB** | Financial Stability Board |
| **G20** | Group of Twenty |
| **GLEIF** | Global LEI Foundation |
| **G-SIBs** | Global Systemically Important Banks |
| **HGG** | Hub Governance Group for the International Data Hub. |
| **ID** | Identification of underlying instrument |
| **IOSCO** | International Organization of Securities Commissions |
| **ISDA** | International Swaps and Derivatives Association |

| | |
|---|---|
| **ISO** | International Organization for Standardization |
| **IT** | Information Technology |
| **LEI** | Legal Entity Identifier |
| **MoU** | Memorandum of Understanding |
| **OTC** | Over-the-Counter |
| **ROC** | Regulatory Oversight Committee for the global LEI system |
| **TR** | Trade Repository |
| **TTP** | Trusted Third Party |
| **UPI** | Unique Product Identifier |
| **UTI** | Unique Transaction Identifier |

# Appendix 8:
# List of References


CPSS-IOSCO: Authorities' access to trade repository data ("Access Report"), August 2013.

CPSS/IOSCO: Report on OTC derivatives data reporting and aggregation requirements ("Data Report"), January 2012.

FSB: A Global Legal Entity Identifier for Financial Markets, 8 June 2012

FSB: OTC Derivatives Market Reforms: Fifth Progress Report on Implementation, 15 April 2013

FSB: OTC Derivatives Market Reforms: Sixth Progress Report on Implementation, 2 September 2013

FSB: OTC Derivatives Market Reforms: Seventh Progress Report on Implementation, 8 April 2014

IMF staff and FSB Secretariat: The Financial Crisis and Information Gaps – Report to the G20 Finance Ministers and Central Bank Governors, October 29, 2009

International Organization for Standardization: ISO 22301:2012 Societal security – Business continuity management systems – Requirements

Regulatory Oversight Committee: Charter of the Regulatory Oversight Committee for the Global Legal Entity Identifier System, 5 November 2012