# Multilateral Framework
## for an
## International Data Hub

### 1. Introduction

1.1 The G-20 finance ministers and central bank governors requested the Financial Stability Board ("**FSB**"), in close consultation with the International Monetary Fund, to improve data collection and sharing with respect to global systemically important financial institutions in order to complement other financial stability policy efforts ("**FSB Data Gaps Project**").

1.2 The purpose of the FSB Data Gaps Project is to increase access to information on the linkages between global systemically important financial institutions and on their common exposures to key sectors and markets in accordance with the mandate provided by the G-20.

1.3 The Bank for International Settlements ("**BIS**") has been asked by the FSB and each of the other signatories hereto to provide the services necessary to act as the international data hub ("**Data Hub**") to facilitate the FSB Data Gaps Project.

### 2. Objective and Scope

2.1 The purpose of this multilateral framework ("**Framework**") is to establish arrangements that will facilitate the collection and sharing of consistent information with respect to Reporting Institutions (as defined below).

2.2 The signatories express their willingness to cooperate and exchange information in good faith in accordance with this Framework.

2.3 This Framework does not create any legally binding obligations or enforceable rights, or modify or supersede any national laws or regulatory requirements in force in the jurisdictions of, or applying to, any of the signatories.

2.4 The signatories may only provide information under this Framework if permitted or not prevented under any laws, regulations, or requirements applying to them.

### 3. Definitions

**Assessment Criteria and Process** means the criteria and process described in **Annex D**.

**Confidential Information** means all Submitted Data, Standard Reports, information received in response to Data Requests, and any other related information or information otherwise held in the Data Hub as agreed by the Governance Group, unless designated as non-confidential by the Governance Group.

**Data Providers** means the entities listed in **Annex B**.

**Data Receivers** means the entities listed in **Annex C**.

**Data Request** means an exceptional request to receive Confidential Information from the Data Hub other than Standard Reports.

**Data Requirements** means the reporting requirements designated by the Governance Group, which will encompass two broad categories of data: institution to institution data on the bilateral exposures of Reporting Institutions ("**I-I Data**") and institution to aggregate data on the exposures of an individual Reporting Institution to aggregates such as countries and financial sectors ("**I-A Data**").

**Framework Parties** means the BIS, entities in the Governance Group, Data Providers, and Data Receivers.

**G-SIFIs** means the institutions designated by the FSB as global systemically important financial institutions, as updated from time to time by the FSB based on the methodology set out by the Basel Committee on Banking Supervision.

**Governance Group** means the group of entities listed in **Annex A**.

**Reporting Institution** means any G-SIFI or other financial institution whose data is being submitted to the Data Hub.

**Standard Reports** means the reports prepared and distributed by the Data Hub in accordance with the form, content, and frequency approved by the Governance Group.

**Submitted Data** means the data submitted by Data Providers to the Data Hub conforming to the Data Requirements.

## 4. Providing data to the Data Hub

4.1 The Data Providers will submit data to the Data Hub conforming to the Data Requirements.

4.2 Each Data Provider has determined that:

4.2.1 the provision of its Submitted Data is consistent with applicable legal and regulatory requirements in its jurisdiction; and

4.2.2 its Submitted Data may be used as described in the Framework, and there is no legal or regulatory requirement in its jurisdiction that would prevent or restrict such use.

4.3 Data Providers will use their best efforts to ensure the accuracy, completeness, and timeliness of the Submitted Data and the Data Hub will provide periodic reports in this regard to the Governance Group. The Data Hub and Data Receivers do not undertake

any responsibility to independently verify the accuracy or completeness of any Submitted Data.

4.4 For operational reasons, data may be submitted on behalf of a Data Provider by another Data Provider in its given jurisdiction, although this will not alter the rights and responsibilities of the Data Provider with respect to the Submitted Data.

4.5 Data provided directly to the Data Hub by Reporting Institutions will not be accepted by the Data Hub and will either be rejected or deleted.

4.6 In cases where there is more than one Data Provider in a given jurisdiction, they will coordinate and exchange information to ensure the smooth and efficient functioning of this Framework arrangement.

## 5. Data Access

5.1 Access to I-I or I-A Confidential Information by Data Receivers in a jurisdiction (initially and on an on-going basis) is contingent on the reciprocal provision of the respective required I-I or I-A Submitted Data by Data Providers in that jurisdiction.

5.2 Data Receivers will ordinarily have access to the Submitted Data only by means of Standard Reports prepared and distributed by the Data Hub.

5.3 The Governance Group will determine the general form and content of the Standard Reports and the frequency of their availability.

5.4 Data Receivers will be given access to the Standard Reports unless their access is restricted under 8.4.

5.5 Data Requests must be submitted to the Data Hub in writing and will only be granted if the Data Hub receives the prior written consent of each Data Provider that provided data covered by the Data Request. Consent may also be granted by a Data Provider on a standing basis. The Data Hub will report any granted Data Requests to the Governance Group.

5.6 Any action taken by any Framework Party on the basis of Confidential Information is the sole responsibility of that Framework Party.

## 6. Data Protection, Confidentiality, and Professional Secrecy

6.1 In all Data Receiver jurisdictions there are rules, regulations, or other enforceable provisions covering data protection, confidentiality, and professional secrecy that the Data Providers have assessed on the basis of the information submitted according to the Assessment Criteria and Process.

6.2 All Confidential Information will be treated by the Framework Parties in a confidential manner at all times to the fullest extent permitted by applicable law.

6.3 All Framework Parties must apply strict standards of data security to Confidential Information and limit the use, processing, storage, transfer and disclosure of such information consistent with the purposes for which the data was provided to the Data Hub and the terms of this Framework.

6.4 Data Receivers may use Confidential Information only within their organizations and only in connection with their respective supervisory activities or macroprudential functions, which include: (i) the analysis and monitoring of interconnectedness among Reporting Institutions; (ii) the identification, monitoring and analysis of risk concentrations; (iii) the development and coordination of macroprudential efforts; and (iv) the development, coordination, and execution of responses in crisis situations.

6.5 Confidential Information received by Data Receivers from the Data Hub or from any other Framework Party may not be shared with others except as provided below.

6.5.1 Before a Data Receiver discloses any Confidential Information, it must request and obtain prior written consent from all Data Providers which provided data for institutions identified in the Confidential Information. Data Providers which are requested by a Data Receiver to permit disclosure will endeavor to respond to that Data Receiver within twenty days. The Data Hub must be informed of all such requests and their resolution.

6.5.2 In the event that a Framework Party is required by statute or legal process to disclose Confidential Information, that Framework Party will, to the extent permitted by law, inform each Data Provider that provided Confidential Information which must be disclosed about such possible compelled disclosure and seek the Data Provider's prior written consent. If the Data Provider does not consent to such disclosure, the Framework Party that is compelled to disclose the Confidential Information will, to the extent possible, seek to preserve the confidentiality of such information and take reasonable steps to resist disclosure, including by asserting such appropriate legal exemptions or privileges with respect to the information as may be available and employing legal means to challenge an order that compels disclosure.

6.6 The foregoing limitation on sharing Confidential Information with others does not prevent a Data Receiver from communicating to a Reporting Institution for which it is the home jurisdiction supervisor concerns raised by or derived from Confidential Information, provided that the identity of any Reporting Institution for which that Data Receiver is not the home jurisdiction supervisor or any other Confidential Information may not be revealed other than in accordance with 6.5 above.

6.7 No privileges, immunities, or confidentiality associated with Confidential Information are intended to be waived as a result of permitting the disclosure of such information under this Framework.

6.8 The Framework procedures and undertakings are intended to govern the treatment of Confidential Information provided pursuant to its terms and should not be deemed to cover or prejudice other types of cooperation that may take place under bilateral or multilateral arrangements between or among Framework Parties.

6.9 This Framework itself is not confidential.

## 7. Data Hub Services

7.1 At the request of the other Framework Parties the BIS agrees to act as the Data Hub by providing the services described in this Framework.

7.2 The BIS has created a specific unit within the BIS dedicated to providing such services, which is not permitted to share the Confidential Information entrusted to it with anyone outside the Data Hub (whether at the BIS or otherwise), other than in accordance with this Framework.

7.3 The Data Hub will store the Confidential Information in a secure environment and access by BIS staff will be restricted to authorised staff who are responsible for the operation of the Data Hub and the related information technology systems, and in compliance, legal, and audit functions, and assigned by BIS management to fulfill these responsibilities.

7.4 BIS staff members are subject to rules and regulations covering data protection, confidentiality, and professional secrecy which the Framework Parties other than the BIS reviewed before entering into this Framework arrangement.

7.5 The BIS has shared with the other Framework Parties the detailed, technical aspects of how the Data Hub will handle the Confidential Information. Any changes to these operating procedures will be subject to the Governance Group's approval.

7.6 The Data Hub will act in good faith with due diligence in preparing the Standard Reports and any responses to Data Requests but cannot guarantee their accuracy or completeness.

## 8. Governance

8.1 The Governance Group is solely responsible for all governance aspects of this Framework arrangement.

8.2 Each jurisdiction represented in the Governance Group is entitled to one vote, regardless of the number of entities within that jurisdiction represented in the Governance Group.

8.3 All jurisdictions represented in the Governance Group must agree by unanimous vote to make any decisions, including to do the following:

- 8.3.1 changing this Framework (including all annexes);
- 8.3.2 admitting a new Data Provider or Data Receiver, including a successor entity of an existing Data Provider or Data Receiver, and including such entity in the Governance Group;
- 8.3.3 changing the Data Requirements, including inclusion of non G-SIFIs as Reporting Institutions; and
- 8.3.4 changing the Standard Reports, including with respect to their general form and content.

8.4 Decisions regarding the continued participation of particular Governance Group members in the cooperation and information exchange contemplated in this Framework, for example, restricting a Data Receiver's access to certain data or reports, or retaining a Data Provider, Data Receiver, or Governance Group member in the Framework

arrangement, must be made unanimously by all jurisdictions represented in the Governance Group other than the jurisdiction(s) of the Governance Group member(s) under consideration.

8.5 The Governance Group may establish advisory groups to aid its work on a temporary or standing basis. The Governance Group cannot delegate any decision-making power to advisory groups. An initial advisory group to advise on the use of Submitted Data and the development of Standard Reports is anticipated.

8.6 The Data Hub will act as the secretariat for the Governance Group.

8.7 The Governance Group will establish its own organizational procedures, including to address any of the following:

8.7.1 the frequency of its meetings;

8.7.2 whether and how to appoint a chair;

8.7.3 how to place an item on the Governance Group's agenda;

8.7.4 voting procedures and mechanics; and

8.7.5 establishing advisory groups and their interaction with the Governance Group.

## 9. Framework - Admission and Withdrawal

9.1 The Governance Group must approve the admission of a Data Provider, Data Receiver, or Governance Group member in accordance with section 8 above.

9.2 The Governance Group may consider a request to become a Framework Party from an entity performing supervisory activities or a central bank or monetary authority with macroprudential functions, which has in its jurisdiction a potential Reporting Institution. The criteria against which the applicant will be assessed are described in the Assessment Criteria and Process.

9.3 Any Framework Party that wishes to withdraw from this Framework must give written notice to the Data Hub as Governance Group secretariat, which will inform the Governance Group and the BIS. If the withdrawing party is a Data Provider, it will stop providing data, and if it is a Data Receiver, the Data Hub will no longer provide Standard Reports or data access to such withdrawing Framework Party as of the date it receives the written notice.

9.4 If a Framework Party that has withdrawn or is not retained wishes to rejoin this Framework, it should apply according to 9.2.

9.5 In the event that the composition of Data Providers, Data Receivers, or Governance Group members is changed, whether by new admissions, withdrawals, due to successor entities of existing members, or otherwise, the relevant Framework annexes will be updated accordingly by the Governance Group without the need for the Framework to be re-signed.

## 10. Transition

10.1 The Data Providers initially signing this Framework are expected to use their best efforts in accordance with 4.3 to submit data fully conforming to the Data Requirements. It is understood, however, that absolute accuracy, completeness, and timeliness of

Submitted Data may take some time to achieve. When a Data Provider submits I-I-Data and/or I-A Data for at least one of the Reporting Institutions in its jurisdiction fully conforming to the Data Requirements, the Data Receiver(s) in that jurisdiction will have access to Confidential Information of the corresponding type, I-I and/or I-A, as specified in this Framework. Such access would be subject to review by the Governance Group twelve months after the Data Provider first receives access.

10.2 By signing the Framework, the Framework Parties agree to the form of the initial Data Requirements and Standard Reports previously provided to each of them. Changes must be agreed by the Governance Group in accordance with section 8.3.

10.3 All Data Providers who subsequently join the Framework arrangement will normally be expected to submit data fully conforming to the Data Requirements for all Reporting Institutions in their jurisdiction at the time they sign the Framework. The Governance Group may grant a new Data Provider a transition period to meet its full reporting requirements. The Governance Group will set the terms of the transitional period at the time that it accepts a new Data Provider into the Framework.

## 11. General Provisions

11.1 This Framework and any future amendments will take effect when the Data Hub informs the Governance Group members it has received signed copies from all expected signatories.

11.2 This Framework may be executed in any number of counterparts, each of which is an original and all of which together evidence the same document.

11.3 This Framework has an indefinite duration.

11.4 The confidentiality provisions in this Framework will continue to apply regardless of whether an entity withdraws from, or is not retained in, the Framework or if the Framework is terminated.

11.5 Any potential changes to this Framework, Data Requirements, Standard Reports, or other aspects which would impact the role of the BIS as the Data Hub will be discussed with the BIS to ensure such changes present no operational or other issues, which would need to be satisfactorily addressed before the changes are put in place. The Governance Group will also inform the FSB Chairman of any such changes which would impact the scope and purpose of the FSB Data Gaps Project.

11.6 No provision of this Framework is intended to give rise to the right of any person, entity or government authority, directly or indirectly, to obtain any information or to challenge the execution of a request for information under this Framework.

11.7 No Framework Party waives any immunity from suit or privilege to which it may be entitled, nor submits to the jurisdiction of any court that would not have been a court of competent jurisdiction if this Framework had not been executed or signed by it.

## Annex A
### Governance Group

**Canada** – Office of the Superintendent of Financial Institutions and Bank of Canada
**France** – Autorité de contrôle prudential and Banque de France
**Germany** – Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) and Deutsche Bundesbank
**Italy** – Banca d'Italia
**Japan** - Financial Services Agency and Bank of Japan
**The Netherlands** – De Nederlandsche Bank
**Spain** – Banco de España
**Sweden** – Sveriges Riksbank and Finansinspektionen (Swedish FSA)
**Switzerland** – Swiss Financial Market Supervisory Authority FINMA and Swiss National Bank
**United Kingdom** – Prudential Regulation Authority and Bank of England
**United States** – Board of Governors of the Federal Reserve System and Federal Reserve Banks and Office of the Comptroller of the Currency

## Annex B
### Data Providers

**Canada** – Office of the Superintendent of Financial Institutions and Bank of Canada
**France** – Autorité de contrôle prudential and Banque de France
**Germany** – Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) and Deutsche Bundesbank
**Italy** – Banca d'Italia
**Japan** - Financial Services Agency and Bank of Japan
**The Netherlands** – De Nederlandsche Bank
**Spain** – Banco de España
**Sweden** – Sveriges Riksbank and Finansinspektionen (Swedish FSA)
**Switzerland** –Swiss Financial Market Supervisory Authority FINMA and Swiss National Bank
**United Kingdom** – Prudential Regulation Authority and Bank of England
**United States** – Board of Governors of the Federal Reserve System and Federal Reserve Banks and Office of the Comptroller of the Currency

## Annex C
### Data Receivers

**Canada** – Office of the Superintendent of Financial Institutions and Bank of Canada
**France** – Autorité de contrôle prudential and Banque de France
**Germany** – Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) and Deutsche Bundesbank
**Italy** – Banca d'Italia
**Japan** - Financial Services Agency and Bank of Japan
**The Netherlands** – De Nederlandsche Bank
**Spain** – Banco de España
**Sweden** – Sveriges Riksbank and Finansinspektionen (Swedish FSA)
**Switzerland** – Swiss Financial Market Supervisory Authority FINMA and Swiss National Bank
**United Kingdom** – Prudential Regulation Authority and Bank of England
**United States** – Board of Governors of the Federal Reserve System and Federal Reserve Banks and Office of the Comptroller of the Currency

## Annex D
## Assessment Criteria and Process

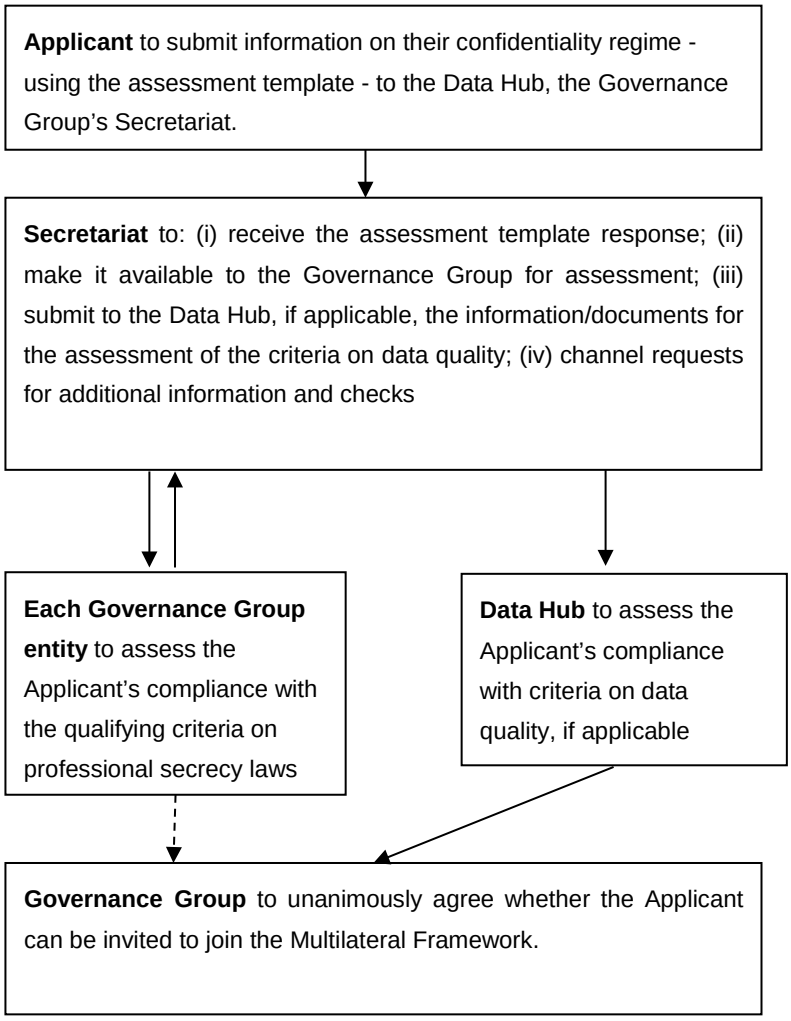
This Annex includes:

- a flowchart with the procedure for the assessments;
- the qualifying criteria; and
- the assessment template;

for the purpose of becoming a signatory to the Multilateral Framework.

### I) Procedure

The following flowchart describes the assessment process for new applicants to the Multilateral Framework:



## II) Qualifying criteria

### Section A – Qualifying criteria for the assessment of professional secrecy laws

### Principle 1 – Existence of professional secrecy obligation

**Objective:** To establish that an on-going obligation of professional secrecy is imposed on all persons who work or have worked, and all auditors or experts acting or who have acted on behalf of the applicant, in respect of information received in the course of their work for or on behalf of the applicant.

| Indicators | Standard Required |
|---|---|
| **Legal requirements** | Specific professional secrecy provisions in the: (i) Legal Framework[1] that are binding in the jurisdiction applying to the applicant and related persons; and/or (ii) contracts between the applicant and related persons. |
| **Applicability - persons** | Professional secrecy obligations must apply to all persons:<br>▪ working or who have worked for the applicant; and<br>▪ acting or who have acted on behalf of the applicant (including all auditors and experts). |
| **Duration of obligation** | Professional secrecy obligation applicable:<br>▪ at all times whilst working for, or acting on behalf of, the applicant; and<br>▪ on an ongoing basis thereafter. |
| **Nature of information** | Professional secrecy obligation applicable:<br>▪ to confidential information received in the course of their work for, or on behalf of, the applicant. |

[1] 'Legal framework' means in this Annex 'the comprehensive legal system for a particular jurisdiction established by any combination of the following: a constitution; primary legislation enacted by a legislative body which has the authority in respect of the jurisdiction; subsidiary legislation made by authorities authorised by the primary legislation for such jurisdiction; policies, practices, or procedures implemented by authorities authorised by the primary legislation for such jurisdiction; and legal precedent and customs applied by the courts.'

**Principle 2 – Definition of Confidential Information**

**Objective:** To establish that the definition of confidential information covers at least the type of information to be shared under the Multilateral Framework being subject to the protection afforded by the Legal Framework to confidential information.

| Indicators | Standard Required |
|---|---|
| **Legal requirements** | Provisions in the Legal Framework which protect confidential information should cover at least the type of information to be shared under the Multilateral Framework. |
| **Nature of information** | Legal Framework regarding confidential information should cover, at least, institution specific information which:<br>▪ has been received in the course of a person's work for or on behalf of the applicant;<br>▪ is not in the public domain; and<br>▪ is not in summary or aggregate form such that individual credit institutions cannot be identified. |

**Principle 3 – Use of confidential information**

**Objective:** To establish that confidential information should only be used by the applicant for supervisory purposes or macroprudential functions.

| Indicators | Standard Required |
|---|---|
| **Performance of supervisory activities or macroprudential functions** | Confidential information received by the applicant should only be used in connection with supervisory activities or macroprudential functions, which include: a) the analysis and monitoring of interconnectedness among financial institutions; b) the identification, monitoring and analysis of risk concentrations; c) the development and coordination of macroprudential efforts; and d) the development, coordination, and execution of responses in crisis situations. |

**Principle 4 – Restrictions on disclosure of confidential information**

**Objective:** To establish that an applicant that receives confidential information in the performance of its duties is allowed to:

- impose restrictions or prohibitions to onward disclosure of such confidential information; and/or
- use its discretion to choose not to disclose such confidential information;

except in relation to cases where the applicant (i) is required by statute or legal process; or (ii) makes disclosure with the consent of the originating entity.

| Indicators | Standard Required |
|---|---|
| **Legal requirements** | Legal Framework allows the applicant to:<br>▪ impose restrictions or prohibitions to onward disclosure of such confidential information; and/or<br>▪ use its discretion to choose not to disclose such confidential information;<br>except in relation to cases where the applicant (i) is required by statute or legal process; or (ii) makes disclosure with the consent of the originating entity. |
| **Specific consent of originating entity** | Where the confidential information originates in another jurisdiction, disclosure may be permitted where:<br>▪ the express prior consent to the disclosure of the information by the entity from which the information originated is obtained by the entity that receives the information; and<br>▪ it is for the purposes for which the originating entity has given its consent. |

**Principle 5: Breach of professional secrecy and disclosure requirements relating to confidential information**

**Objective:** To establish that disclosure of confidential information in breach of the obligation of professional secrecy by any person bound by the obligation is unlawful and sanctionable.

| Indicators | Standard Required |
|---|---|
| **Legal requirements** | Provisions in the Legal Framework in respect of the breach of professional secrecy obligation, comprising of:<br>▪ offences<br>▪ penalties |
| **Enforcement process** | Provision in the Legal Framework relating to enforcement powers in respect of the breach/threatened breach of the professional secrecy obligation. |

| | |
|---|---|
| | Evidence of previous relevant and successful enforcement action, if any. |

**Section B – Qualifying criteria for the assessment of data quality**

**Principle 6: Data quality assurance**

**Objective:** To establish that the applicant controls the quality of information transmitted to the Data Hub, if applicable.

| Indicators | Standard Required |
|---|---|
| **Control procedures** | The applicant should have procedures for assuring, on a best efforts basis and prior to transmission to the Data Hub, that the accuracy, completeness and timeliness of information transmitted to the Data Hub meet the standards agreed by the signatories to the Multilateral Framework. |
| **Nature of information** | Data quality assurance procedures should apply to quantitative and qualitative information transmitted to the Data Hub, comprising:<br>▪ institution-to-institution data<br>▪ institution-to-aggregate data |

**Principle 7: Data quality queries**

**Objective:** To establish that the applicant reviews and corrects, if necessary, information transmitted to the Data Hub, if applicable.

| Indicators | Standard Required |
|---|---|
| **Feedback procedures** | Resources should be available at the applicant to answer queries related to the accuracy, completeness and timeliness of information transmitted to the Data Hub. |
| **Revision procedures** | Resources should be available at the applicant to review and correct, if necessary, information transmitted to the Data Hub. |

**III) Assessment Template:**

**Template for the assessment of the applicant's confidentiality provisions**

**General instructions:**

Please provide a complete response to each question, and copies of the laws, rules and regulations that support each response.

The responses and the accompanying material (including laws, rules and regulations) should be provided in English and sent to the Data Hub.

This template will be reviewed with the qualifying criteria for becoming a signatory to the Multilateral Framework.

This assessment template was prepared by: [insert contact details of the author].

**NAME OF COUNTRY:**

**NAME OF AUTHORITY (the 'Applicant'):**

**SECTION A – QUALIFYING CRITERIA FOR THE ASSESSMENT OF PROFESSIONAL SECRECY LAWS**

**PRINCIPLE 1 – EXISTENCY OF PROFESSIONAL SECRECY OBLIGATION**

1. **Please identify and explain the provision(s) in the Legal Framework and/or in contracts that establish a professional secrecy obligation on all persons that receive confidential information: (i) working or who have worked for the Applicant; and (ii) acting or who have acted on behalf of the Applicant (including all auditors and experts)?**
2. **Please identify and explain the provision(s) in the Legal Framework and/or in contracts which state that the professional secrecy obligation applies: (i) at all times whilst working for, or acting on behalf of, the Applicant; and (ii) on an ongoing basis thereafter?**

**Assessment of equivalence with the qualifying criteria regarding the existence of professional secrecy obligation:**

**PRINCIPLE 2: DEFINITION OF CONFIDENTIAL INFORMATION**

3. **Please identify the provision(s) in the Legal Framework which protect confidential information and explain whether they cover at least the type of information to be shared under the Multilateral Framework that: (i) has been received in the course of a person's work for or on behalf of the Applicant; (ii) is not in the public domain; and (iii) is not in summary or aggregate form such that individual credit institutions cannot be identified.**

| |
|---|
| |
| **Assessment of equivalence with the Qualifying Criteria regarding the definition of confidential information:** |
| |
| **PRINCIPLE 3: USE OF CONFIDENTIAL INFORMATION** |
| **4. Please identify and explain the provision(s) in the Legal Framework that restrict the use of confidential information received by the Applicant for supervisory activities or macroprudential functions.** |
| |
| **Assessment of equivalence with the qualifying criteria regarding the use of confidential information:** |
| |
| **PRINCIPLE 4: RESTRICTIONS ON DISCLOSURE OF CONFIDENTIAL INFORMATION** |
| **5. Please identify and explain the provision(s) in the Legal Framework that allow the Applicant to impose restrictions or apply its discretion to prevent onward disclosure of such confidential information.**<br>**6. Please identify and explain the provision(s) in the Legal Framework that describe under what circumstances (e.g. to comply with a statute or court order etc) and to whom (e.g. other agencies, courts, legislative bodies etc) the Applicant is legally required to disclose confidential information.** |
| |
| **Assessment of equivalence with the qualifying criteria regarding restrictions on the disclosure of confidential information:** |
| |
| **PRINCIPLE 5: BREACH OF PROFESSIONAL SECRECY AND DISCLOSURE REQUIREMENTS RELATING TO CONFIDENTIAL INFORMATION** |
| **7. Please identify and explain the provision(s) in the Legal Framework that establishes that unlawful breach of professional secrecy and disclosure requirements can lead to sanctions being imposed on any person bound by such obligation.**<br>**8. Please provide details of the maximum sanctions that can be levied on such person(s) (e.g. fines or imprisonment) and evidence of any relevant and successful enforcement action and actual sanctions levied in respect of the breach/threatened breach of the professional secrecy obligation.** |
| |

| |
|---|
| **Assessment of equivalence with the qualifying criteria regarding the breach of professional secrecy and disclosure requirements relating to confidential information:** |
| |
| **SECTION B – QUALFYING CRITERIA FOR THE ASSESSMENT OF DATA QUALITY** |
| **PRINCIPLE 6: DATA QUALITY ASSURANCE** |
| **9. Please, if applicable:**<br>**(i) explain the procedures set up to ensure the accuracy, completeness and timeliness of the data; and**<br>**(ii) provide to the Secretary for assessment by the Data Hub a set of sample of real data for two consecutive reporting periods for the purpose of testing these procedures and not for sharing with signatories to the Multilateral Framework.** |
| |
| **Assessment of equivalence with the qualifying criteria regarding data quality:** |
| |
| **PRINCIPLE 7: DATA QUALITY QUERIES** |
| **10. Please explain the procedures set up and the resources available to review and to correct (if necessary) the accuracy of the data, if applicable.** |
| |
| **Assessment of equivalence with the qualifying criteria regarding data quality:** |
| |

## Document history

| Version | Date | Changes |
|---|---|---|
| 1.0 | 28 March 2013 | n/a |
| 1.1 | 10 June 2013 | UK PRA replaces UK FSA as successor entity in Annexes A, B, and C |
| 2.0 | 2 April 2014 | Phase 2 changes to include four Data Provider central banks as Data Receivers (BoC, BdF, SNB, BoE) |
| 2.1 | XX April 2015 | Sveriges Riksbank and Finansinspektionen added as Governance Group members, Data Providers and Data Receivers in Annexes A, B and C |

**Bank for International Settlements (BIS)**

Date: _____

| | |
|---|---|
| Name: | Name: |
| Title: | Title: |

Canada

**Office of the Superintendent of Financial Institutions (OSFI)**

Date: _____

_____

Name:
Title:

**Bank of Canada**

Date: _____

_____

Name:
Title:

France:

**Autorité de contrôle prudential (ACP)**

Date: _____

_____

Name:
Title:

**Banque de France**

Date: _____

Name:
Title:

Germany:

**Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)**

Date: _____

| | |
|---|---|
| Name: | Name: |
| Title: | Title: |

**Deutsche Bundesbank**

Date: _____

| | |
|---|---|
| Name: | Name: |
| Title: | Title: |

Italy:

**Banca d'Italia**

Date: _____

_____

Name:
Title:

Japan

日本銀行 **Bank of Japan**

Date: _____

Name:
Title:

金融庁 **Financial Services Agency**

Date: _____

| | |
|---|---|
| Name: | Name: |
| Title: | Title: |

The Netherlands:

**De Nederlandsche Bank**

Date: _____

_____

Name:
Title:

Spain:

**Banco de España**

Date: _____

Name:
Title:

Switzerland:

**Swiss Financial Market Supervisory Authority FINMA**

Date: _____

| | |
|---|---|
| Name: | Name: |
| Title: | Title: |

**Swiss National Bank**

Date: _____

| | |
|---|---|
| Name: | Name: |
| Title: | Title: |

United Kingdom:

**Prudential Regulation Authority**

Date: _____

_____

Name:
Title:

**Bank of England**

Date: _____

Name:
Title:

United States:

**The Board of Governors of the Federal Reserve System**

Date: _____

_____

Name:
Title:

**Office of the Comptroller of the Currency**

Date: _____

_____

Name:
Title:

Sweden:

**Finansinspektionen (Swedish FSA)**

Date: _____

| | |
|---|---|
| Name: | Name: |
| Title: | Title: |

**Sveriges Riksbank**

Date: _____

| | |
|---|---|
| Name: | Name: |
| Title: | Title: |