September 28, 2012

Comments on the Basel Committee on Banking Supervision's Consultative Document:
Principles for effective risk data aggregation and risk reporting

Japanese Bankers Association

We, the Japanese Bankers Association ("JBA"), would like to express our gratitude for this opportunity to comment on the consultative document: Principles for effective risk data aggregation and risk reporting, released on June 26, 2012 by the Basel Committee on Banking Supervision (the "Committee").

While understanding the purposes of the principles set forth in this consultative document, we respectfully expect that the following comments will be considered based on those proposed principles.

[General Comments]

1. Supervisory expectations should be feasible.

In providing supervisory expectations associated with the proposed principles, we respectfully request that the contents of such expectations should be feasible, taking into consideration that the IT resources of financial institutions are limited. Financial institutions are currently investing a considerable amount of IT resources in order to address a variety of regulations, such as Basel III (including liquidity requirements) that are effective from and after January 2013. In addition to this, there is a concern that common data templates for global systemically important financial institutions (G-SIFIs) may also require them to develop a large-scale system within a short time frame, depending on the contents agreed in the near future.

As noted in Paragraph 9, it is well understood that "the long-term benefits of improved risk data aggregation capabilities and risk reporting practices will outweigh the initial investment costs incurred by banks". However, the implementation of various new regulations is underway, with a target of achieving the stated objectives within a few years. Under such a situation, in the short run, initial investment costs associated with data and system developments may only pile up. Multifaceted comments are provided in the

Specific Comments below, but, as a general overview comment, supervisors should provide feasible expectations, taking into account the limitation on IT resources of respective financial institutions.

The proposed principles should allow a bank itself to defines, collects and processes (sorts, consolidates and classifies) “risk data”, which is a first step of a series of improved risk data aggregation capabilities and enhanced risk reporting practice. This will facilitate communications between supervisors and banks and enable the supervisors to achieve more effective supervision.

2. Time frame (timelines and transitional arrangements) should be practicable.

The consultation requires national supervisors to start discussing implementation of the principles with senior management G-SIBs in early 2013 (Paragragh 18). In 2013, the supervisors would require self-assessments by G-SIBs (Paragragh 75) and the committee would start observations on the effectiveness of the principles (Paragragh 19). Also, a bank board and senior management would be required to have a strategy to meet the principles by 2016 at the latest (Paragragh 20). However, the timeframe would be modified to be more feasible since it is necessary for each financial institution to set a sufficient duration for preparation. For details, see “5. Timelines / transitional arrangements” of “[Specific Comments]” described later.

3. A framework should place priority on the judgments of national supervisors.

The concept underlying throughout the consultative document appears to be on a principle basis. However, there is a concern that, through assessment by harmonisation among national supervisors, these principles may, in effect, be translated into more conservative “rules” than initially intended. We therefore respectfully request that a framework that emphasizes judgments made by national supervisors based on each bank’s circumstances as noted in this consultative document should also be retained in the final text.

4. Duplicated principles should be eliminated.

Some of the principles set out in this consultative document seem to be similar or duplicative, and it is therefore preferred that such principles be consolidated in light of the purposes and effectiveness of each principle.

For example, “II. Risk data aggregation capabilities” and “III. Risk reporting practices” specify “Accuracy” requirements in Principles 3 and 7, respectively. As accurate reporting and accurate data aggregation are inseparable, both should be treated as one single principle. The same applies to the relations between Principle 4 “Completeness” and Principe 8

"Comprehensiveness", and between Principle 5 "Timeliness" / Principle 6 "Adaptability" and Principle 10 "Frequency". In particular, the only difference between Principle 5 "Timeliness" and Principle 6 "Adaptability" in "II. Risk data aggregation capabilities" is whether the reporting request is ad-hoc or not, and hence the usefulness of separating these two principles is considered to be limited.

Further, Principle 11 "Distribution" should be included in Principle 1 "Governance". It is not considered necessary to separately set out Principle 11. Similar or duplicative principles may cause the purpose of each principle to be unclear, and may impair their effectiveness.

5. Trade-offs between the principles should only be prohibited if such Trade-offs will materially inhibit risk management decisions.

We understand that trade-offs are inherent in all of the proposed principles listed in this consultative document. We therefore express our dissenting voice to denying trade-offs as stated in Paragraph 17. In particular, it is generally known that there is a negative correlation between accuracy/completeness and timeliness. Thus, it is requested that the final document contains a statement to the effect that "While understanding that the trade-offs may exist, such trade-offs should not materially inhibit risk management decisions". A message should imply that the requirements of risk management and financial supervision are required to be met, in light of an actual situation, without falling into idealism and doctrinism.

For example, a requirement to simultaneously meet all principles, including Principle 3 "Accuracy and Integrity", Principle 4 "Completeness" and Principle 5 "Timeliness", would be an excessive expectation. Notably, as required by Principle 5 that "……The precise timing will depend upon the nature and potential volatility of the risk being measured as well as its criticality to the overall risk profile of the bank", it is evident that simultaneously meeting these principles in any circumstances is not realistic. Furthermore, simultaneously meeting Principle 7 "Accuracy", Principle 8 "Comprehensiveness" and Principle 10 "Frequency" would be an excessive expectation as described later.

[Specific Comments]

Scope and initial considerations:

(1) Application at both the banking group and on a solo basis

Paragraph 11 stipulates that the principles should apply at both the banking group and on a solo basis, but supervisory expectations should be developed for each level in the banking

group (e.g. the holding company, the individual banking group and the solo bank). It is reasonable to assume that supervisory expectations differ at each level of the consolidation scope. Accordingly, it is not necessary to require all the level apply the principles including IT infrastructure developments in the same way. For example, in cases where consolidated subsidiaries within a group have no material risk or where their impact on risk is immaterial, it is requested that risk management data on a solo basis be accepted, since such cases have a limited adverse impact on the stability of individual banks and financial system as a whole.

(2) “Forward-looking” data

Clarification of what “forward-looking” risk data noted in Paragraph 12 means would be appreciated.

Some data do not meet the principles of accuracy, integrity, comprehensiveness, and completeness, etc., or do not need to meet them. If results of stress testing and forecasted credit costs are assumed as “forward-looking” data, the necessity of requiring these data could be understood to some extent. However, these are merely forecasts and should not be required to satisfy requirements of accuracy, integrity, comprehensiveness and completeness.

I. Overarching governance and infrastructure

Principle 1: Governance

Paragraph 22 (a) states that “Independent validation could mean a review by the internal audit function. However, best practice would suggest that an independent validation unit with specific IT, data and reporting knowledge may be better positioned to perform this review”. This description implies the establishment of a new business unit independent of both the function actually making risk reports and the internal audit function, but the intention of such statement is unclear. It is therefore requested to specify a reason why a review by the internal audit function is determined to be insufficient, as well as to confirm whether, if an outsourced review by an external specialist would be acceptable as the independent validation.

Paragraph 22 (b) stipulates that “When considering a material acquisition, a bank’s due diligence process should assess the risk data aggregation capabilities and risk reporting practices of the acquired entity, as well as the impact on its own risk data aggregation capabilities and risk reporting practices. The impact on risk data aggregation should be considered explicitly by the board and inform the decision to proceed”. In order to specify

that the consideration requirement should depend on the materiality, this description should be changed to "The impact on risk data aggregation should be considered by the board, subject to materiality".

Similarly, Paragraph 23 notes that "A bank's board and senior management should be fully aware of any limitations that prevent full risk data aggregation, in terms of coverage, in technical terms or in legal terms". The description "should be fully aware of any limitations" could be construed as being an excessive expectation for the board and senior management, and hence this requirement should be narrowed.

Principle 2: Data architecture and IT infrastructure

With respect to Paragraph 24, risk data aggregation capacities and risk reporting practices constitute the basis for supporting a bank's business execution, but these alone are insufficient to support the analysis of the impact on the bank's business. The analysis of the impact on the bank's business can only be completed in combination with such information as profitability and positioning on the relevant business. Business planning and strategic decision-making can only be delivered through a combination of these.

Further, with respect to Paragraph 25, data taxonomies and architecture are determined along with data models, based on the concept of a bank's system architecture, and accordingly system integration is not necessarily requisite. Whether to develop an integrated-type or distributed-type system should be decided in accordance with each bank's policies, and integration should not be mandatory. Most banks may chose the option of an integrated architecture as a result; however, even if a distributed-type system is selected, it would be possible to maintain high data aggregation capacities by building an interface equipped with a robust conversion function.

In addition, Footnote 10 mentions "rather, there should be robust automated reconciliation procedures where multiple models are in use". Reconciliation procedures between different data models are necessary, but "automated" reconciliation procedures should not be mandatory since what is essential is the appropriate balance between "automated" and "manual" procedures as stated in Paragraph 30.

II. Data aggregation capabilities

Principle 3: Accuracy and Integrity

(1) Automated data aggregation

Principle 3 stipulates that “Data should be aggregated on a largely automated basis so as to minimise the probability of errors.” Given that it is not practical to automate all the data aggregation processes, the principle itself should also add that “There should be an appropriate balance between automated and manual systems,” as mentioned in Paragraph 30.

Whether to automate a data aggregation process should be determined based not only on professional judgments but also with regards to the materiality including the number of transactions and size of exposure. From this point of view, “important processes which have a significant impact on business” should be subject to automation, rather than “many other processes” as Paragraph 30 sets out.

If a data aggregation process is automated, the amount of manual data reconciliations should be reduced provided that data definitions are clarified and the accuracy of systems is verified during the course of the automation processes.

(2) Clear definition of accuracy and integrity

Accuracy and integrity should be clearly defined.

Accuracy and integrity in a literal sense appear to be impractical as risk data should not always be accurate and integral. Depending on the type and purpose of use of the aggregated data, in some cases, “approximates” (eg in 100 million yen, and in million dollars) or “estimates” may be effective enough for risk management purposes. In addition, as discussed in Principle 6 “Adaptability”, approximates can serve the expected purpose in cases where a bank needs to generate aggregated risk data to meet time-constrained ad hoc requests during crisis situations etc.

(3) Ensuring controls surrounding risk data to be as robust as those applicable to accounting data

Risk data can be based on daily flash summary reports - particularly for internal management purposes - whereas accounting data is based on quarterly settled figures (reflecting financial closing process) which are in compliance with accounting standards. In other words, the requirements for aggregating risk data and those for accounting data differ. Therefore, it is not practical to require controls surrounding risk data to always be as robust as those applicable to accounting data as stipulated in paragraph 28 (a). The required level

of robustness should vary in accordance with the type, nature and use of purpose of risk data.

Further, a more detailed definition on “robust controls” would be appreciated.

(4) Reconciliation to a bank’s sources and books of record

While paragraph 28 (c) stipulates that “Risk data should be reconciled to accounting data, as well as to a bank’s sources and books of record, to ensure that the risk data is accurate,” the data computed by use of models is difficult to be reconciled to accounting data. As not all risk management data is managed in sync with accounting data, practically, there are cases such as risk assets, economic capital, and PE, BPV or VaR of derivatives, where no relevant accounting data for reconciliation exists.

Furthermore, there are many procedures specific to accounting which are not aligned with transactions or risk management procedures. Therefore, various approaches to ensure the accuracy of risk data should be allowed to the extent such approaches are practicable, rather than limiting the option only to the reconciliation to accounting data. For example, if no issue is identified through the verification of the applied model, the accuracy of risk data can be considered to be ensured.

Principle 4: Completeness

We support the statement made in Paragraph 35 “Where risk data is not entirely complete, the impact should not be critical to the bank’s ability to manage its risks effectively”.

While a bank needs to capture and aggregate all material risk data across the banking group, the required level of the completeness of risk data should vary depending on their business model. Investment banks, for example, are more involved in derivatives and securitization whereas commercial banks primarily engage in lending activities. They are exposed to different risks due to such a difference in their asset portfolio. Given this, it is assumed that the level of meeting the principles will vary according to a bank’s business model. Likewise, within the banking group, the level of meeting risk data aggregation required for those affiliates with less significance should be different from other affiliates.

To maintain consistency with other descriptions under Principle 4, the first sentence of Paragraph 35 should be amended by adding the word “materially”: specifically, change it from “…risk data that is complete and …” to “…risk data that is materially complete and…”

Principle 5: Timeliness

Paragraph 38 (b) "Counterparty credit risk exposures" should be amended to "Counterparty credit risk exposures to a large corporate borrower on the supervisory watchlist, including, for example, derivatives," adding the expression used in Paragraph 38 (a) "The aggregated credit exposure to a large corporate borrower on the supervisory watchlist." Banks are required to produce aggregated risk data in a timely manner for those large exposures critical for risk management purposes. Therefore, there is no need to require the aggregation of all exposures only for the counterparty credit risk. Consistency with Paragraph 38 (a) is also requested.

Further, we agree with the consultative document's statement "Banks need to build their risk systems to be capable of producing aggregated risk data rapidly during times of crisis for all critical risks." However, for assets whose exposures do not fluctuate in normal times, we respectfully request the Committee to allow banks to aggregate risk data pertaining to such assets over a certain period.

Principle 6: Adaptability

Paragraph 39 stipulates that "A bank's risk data aggregation capabilities should be…forward-looking to assess emerging risks." As it is unclear from this statement what the principle exactly intends to require, more clarification of this capability is requested for better understanding (eg by providing specific examples).

With regard to the "capabilities to incorporate new developments on the organisation of the business and/or external factors" and "capabilities to incorporate changes in the regulatory framework" which are set out as an example of adaptability in Paragraph 40 (c) and (d) respectively; specific conditions should be set to limit the scope of such capabilities, because systems cannot always address all "changes" depending on their size and extent. It should be understood that capabilities of systems, however sophisticated, are inherently limited.

As for the risk reporting practices discussed in Paragraph 42, the consultative document states that "supervisors expect banks to consider accuracy requirements analogous to accounting materiality (Principle 7: Accuracy)" and requires comprehensiveness in Principle 8. However, during crisis situations, it is vital to focus on the very issues facing the crisis (eg exposures related to the Lehman Brothers and other investment banks at the time of Lehman crisis); and the speediness and frequency of the reporting of such crisis issues should take priority over accuracy and/or comprehensiveness. While it is a matter of

course to make best efforts to ensure accuracy, it would be difficult to meet accuracy requirements analogous to accounting materiality. Rather, “appropriateness” should be considered in discussing accuracy/comprehensive of risk management reports during the times of crisis.

III. Risk reporting practices

Principle 7: Accuracy

As the principles 7 through 11 contradict one another, it is considered impossible to satisfy all the principles at the same time. In respect of risk reporting practices, the accuracy or comprehensiveness of data sources and timeliness have trade-off relationships. Therefore, requiring full compliance with Principle 7 (Accuracy), Principle 8 (Comprehensiveness) and Principle 10 (Frequency) is considered to be an excessive expectation. An alternative approach that allows prioritization of the principles based on materiality (eg a flash summary report which emphasizes speediness) should be permitted and stipulated as such.

Principle 10: Frequency

It is difficult to set a requirement on the reporting deadline in crisis situations. Given the difficulty of projecting crisis situations beforehand, it is not reasonable to predefine the reporting deadline at the time of crisis. Instead, it is considered effective to prepare for crisis by understanding in advance to what extent a bank can obtain reliable data within a shorter time frame than in normal times.

IV. Supervisory review, tools and cooperation

Principle 13: Remedial actions and supervisory measures

Paragraph 67 mentions that “Such tools may include…the possible use of capital add-ons as both a risk mitigant and incentive under Pillar 2.” A further explanation would be appreciated to clarify what specific actions are contemplated for “the possible use of capital add-ons”. Further, consideration should be given to avoid applying excessive requirements.

Paragraph 68 states that “…where deficiencies in data aggregation are assessed as causing significant weakness in risk management capabilities.” This needs to be detailed to specify when deficiencies are “assessed as causing significant weakness.”

Paragraph 69 stipulates that “For new business initiatives, supervisors may require that robust risk data aggregation capabilities are demonstrated before allowing a new business

venture or acquisition to proceed." Please confirm whether our understanding that what a bank should explain to supervisors is "the bank's plan to integrate and align the risk data aggregation capabilities and risk reporting practices of the acquired company within its own framework" is correct. It is not realistic to require banks to demonstrate, at the stage of the application for acquisition to supervisors, that the acquired company has robust risk data aggregation capabilities and risk reporting practices. Therefore, it is considered reasonable to require banks to explain, within the established timeframe, the bank's plan, as stipulated in paragraph 22 (b).

Principle 14: Home/host cooperation

Paragraph 73 stipulates that "Supervisors should discuss their experience regarding the quality of risk data aggregation capabilities and risk reporting practices in different parts of the group." What does the "parts" represent in this context? (Does it mean "offices" or "entities" within a group?) It is requested to clearly define the scope of discussion between home and host supervisors.

Further, please confirm whether this paragraph intends to require the self-assessment of risk data aggregation capabilities and risk reporting practices for each base or entity.

5. Timelines / transitional arrangements

(1) National supervisors starting discussions on implementation of the principles in early 2013

Paragraph 18 states "National banking supervisors will start discussing implementation of the principles with senior management G-SIBs in early 2013". Such discussions require sufficient preparation period in order for financial institutions to carry out self-assessments. It is hence requested that a preparation period of at least six months after the announcement of finalized principles and release of answers to public comments on this document should be ensured.

(2) G-SIBs self assessment of the implementation progress to be made in 2013

Paragraph 75 states "Supervisory approaches are likely to include requiring self-assessments by G-SIBs against these expectations in early 2013". It is requested that these self-assessments be specified by providing illustrations beforehand such as what are assessment standards that will be applied to such self-assessments. The level of implementing the principles may significantly vary depending on factors such as business model, risk profile and risk appetite of each bank, and hence it would be difficult to carry out self-assessments in a uniform manner. In other words, self-assessments need to be conducted taking into account each financial institution's situation, and the appropriate

level of meeting the principles is difficult to determine.

Further, paragraph 74 sets out that “Supervisors expect that a bank’s data and IT infrastructures will be enhanced in the coming years”. Banks are obliged to promote system developments and improvements to address new regulations, such as Basel III and over-the-counter derivatives requirements, in the coming years, resulting in a shortage of human resources at both bank and system developers. For banks, it is a very challenging task to strengthen IT infrastructure in the coming years. As such, it is requested that “in the coming years” be changed to “within the agreed deadline considering each bank’s situation”. For purposes of enhancing data and IT system, the establishment of a realistic timeline would be necessary.

(3) G-SIBs progress to be tracked from 2013

It should be specified that if the G-SIBs progress to be tracked from 2013 as stated in Paragraph 19 results in any revisions to the principles, the timeline of complying with such revisions will be separately set. As G-SIBs will develop a strategy based on the current proposed principles, revisions to the principles may require re-consideration of a strategy. In such cases, it is requested to exempt full compliance by early 2016 for the revised parts.

(4) Developing a strategy to meet the principles by 2016

Paragraph 20 in this consultative document requires banks to develop a strategy to meet the principles by 2016. Certain considerations for feasibility of the strategy development should be made, reflecting the progress of IT infrastructure investment in each jurisdiction. Additionally, paragraph 7 states that “National supervisors expect G-SIBs to implement these principles by 2016”. The level of implementing the principles should vary according to the business model, risk profile and risk appetite of each bank. We therefore request that this requirement should be changed to “National supervisors expect G-SIBs to implement the principles by 2016 to the extent agreed-upon, considering each bank’s situation”.