Consultation Response

Consultation on Draft Regulatory Technical Standards concerning operational risk (EBA/CP/2024/13)

September 2024

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to comment on the EBA's **Consultation on Draft Regulatory Standards concerning operational risk (EBA/CP/2024/13)**. AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia.

AFME is registered on the EU Transparency Register, registration number 65110063986-76.

We summarise below our over-arching comments in relation to the consultation, which is followed by answers to the individual questions raised.

Comments and observations:

The proposals in the consultation paper in relation to the change in taxonomy are broader than expected and could have a significant impact on institutions' management of operational risk if they are maintained. In particular we would like to highlight our concern on the breadth of change considering the mandate under Article 317(9) of the CRR3. The provision empowering the EBA to produce an operational risk taxonomy states clearly:

"9. For the purposes of paragraph 7, EBA shall develop draft regulatory technical standards establishing a risk taxonomy on operational risk that complies with international standards and a methodology to classify the loss events included in the loss data set based on that risk taxonomy on operational risk."

The divergences noted from the recognized international standard provided by the BCBS would, in our strong view, not be in-keeping with the mandate to the EBA of establishing a taxonomy that complies with this standard. We believe that the EBA should re-propose its draft RTS to provide for a taxonomy that is in line with the existing BCBS operational risk taxonomy.

We note in particular that the EBA does not appear to be working in collaboration with the BCBS or other international regulators which is likely to lead to heterogeneity and fragmentation in the management and reporting of operational risk. The absence of global consensus would require international banks to maintain various taxonomies at the same time depending on the region, which would be extremely costly in terms of time and resources and add significant challenges to the management of risk. It would mean for example that a Level 1 historical event could be reported in different ways across jurisdictions, with the possibility of an event being considered in a variety of ways depending on whether it is classified in Europe, or the US and Asia.

The proposed taxonomy diverges in the Level 1 from the BCBS taxonomy, as some definitions are changed from BCBS definitions, therefore as mentioned contradicting the CRR3 mandate, and it has not been mapped or referenced to BCBS Levels 2 and 3.

There is significant concern that the implementation of the proposed taxonomy, while being very costly, may not be definitive or final. It is possible that the BCBS may present another proposal in the coming years which would be likely to involve further adjustments to the EBA's current proposal.

The risk taxonomy is key for managing operational risk in general, and not only for capturing or classifying losses, and we are concerned that some of the changes that are being proposed may not be useful for this essential purpose, for example, the split of some risk types according to intentionality, or the use of some attributes that could change in the future such as large loss events. It would be helpful to understand how the EBA is proposing to use the taxonomy, the extent of the envisioned requirements for reporting, as well as how it will relate to the future RTS on the operational risk management framework (mandate of CRR 3 Article 323(2)).The proposals do not consider sufficiently the scale of the work involved for banks to implement a new risk taxonomy. It would be very important that banks have sufficient time to implement changes in taxonomy, and we consider that it would take at least two years to allow banks to adjust the processes and systems they currently have in place in order to start categorising new operational risk losses as per the new taxonomy. These implementation challenges would only increase with international fragmentation exacerbated by the risk of banks having to rollout and operate more than one regulatory taxonomy for operational risk.

We would in addition note that many banks already have comprehensive and granular operational risk management frameworks and taxonomies and the introduction of the new taxonomy will create significant challenges around the comparability of historic data for internal purposes as well as in relation to regulatory reporting and disclosure, and for the comparability of data between group entities or institutions in general both inside and outside of the EU. While the consultation paper proposes that the new taxonomy would be applicable to events with an impact of greater than €20k in practice banks will often apply lower thresholds, for example in relation to fraud, and the impact of the proposals would accordingly be more significant.

The proposed taxonomy further exacerbates the mix and overlap of causes with event types, and introduces attributes/ flags, thereby moving us further away from a mutually exclusive classification of loss events. This could result in the adoption of divergent practices across banks for selecting risk types and flags, making it challenging to compare data across the industry.

Finally, we are concerned with some of the features of the proposed taxonomy, including the 'intentionality' of the event. It is a very relevant change in paradigm. The rationale for the introduction of the concept of 'intention' is not clear and it requires a burdensome procedure for its implementation, with the analysis of events one by one and the identification of compelling evidence, without a clear output or benefit that offsets the cost for entities. In addition duplicating a risk by possible causes would not help to have a global view on a risk.

Question 1: Do you think that the granularity of and the distinction between the different Level 2 categories is clear enough? If not, please provide a rationale.

The industry would like to raise some concerns on the granularity of and the distinction between the different Level 2 categories.

In the case of Level 1, some definitions are changed from BCBS definitions, which means that the EU level 1 category does not exactly fit with the BCBS Level 1 category. In addition, the changes at Level 2 also affect the definition of Level 1, further diverting from BCBS. This will require large international groups that have operations outside the EU to maintain different taxonomies at the same time. It also raises the issue of a lack of comparability between the BCBS categories from EU and non-EU based institutions, and there appears no rationale for this.

The proposed taxonomy (risk categories and attributes) includes a mixture of risk types, causes and control failures as well as other reporting dimensions including loss type (i.e. pending losses), business line etc.. Some Level 1 categories appear to be very granular in Level 2 (for example, internal fraud) while others are kept at a higher level (for example, employment practices or damage to physical assets).

In relation to Level 1 categories, certain risk types (i.e., Model risk, IT risk, Financial Crime) have been split between various Level 1 categories, based on different criteria. .

One of these criteria is the intentionality of the event (for example, in Financial Crime risks assigned to either Internal Fraud or CPBP Level 1, based on intentionality. The rationale for the introduction of the concept of "intention" is not clear, and it would require a burdensome procedure for implementation without a clear output. We would note that the reporting of intent requires the analysis of events one by one and the identification of compelling evidence. In practice, this may not often occur and when it does it will be subject to assessment and decision making procedures.

We are therefore not supportive of the introduction of the 'intention' feature that introduces instability to the loss data set, with certain losses being subject to potential changes to their categorisation and requiring institutions to devote time and resources with no clear output. There may also be significant legal risks to banks in seeking to classify the actions of its employees as intentional or not. If it was to be introduced at all, then the most appropriate way to proceed would be to consider it an attribute, and to provide banks with clear instructions of how and when to assign this flag.

Another example where a principal risk has been split is IT risk:

> "Business Disruption and System Failures Level 1 risk" does not cover IT failures related to management transactions, which would be classified as Execution, Delivery & Process Management. In the BCBS standard, all systems failures would be considered in BDSF Level 1. Whether IT failures are related to the management of transactions or not, there should not be a different handling in Level 1 event type.

In relation to Level 2 categories, we would have the following comments:

- **Internal Fraud**:
    - In Internal Fraud, 1.4 and 1.5 distinguish between fraud against stakeholders and against the bank, overlapping 1.1, 1.2, 1.3, 1.6, 1.7 and 1.8, which would also qualify as 1.4 and 1.5.
    - We see category 1.7 (International sanctions violation) as a subcategory of 1.8 (Intentional money laundering and terrorism financing).
    - In Internal Fraud, the intentional mismarking may be considered as an event, but it is difficult to quantify the potential impact in losses. We think that this Level 2 item is not significant enough to require a subcategory.
    - "Malicious physical damages to employees": clarifications would be needed as to whether internal fraud is considered under the Level 2 classification as a physical damage caused to employees and not a damage caused by an employee that damages the company's physical assets.

- The "misconduct" approach considers the responsibility of the group and not only the individual responsibility of its employees. This internal impact is not considered in this taxonomy, which is therefore not aligned with the RTS definition (article 4, paragraph 52a, point (d) of Regulation (EU) 575/2013).
- "Insider trading not on institution's account": would also need to be clarified. We understand that it refers to trading on own/personal account.
- There are doubts related to where "Rogue Trading" would be classified.

- **External Fraud**:
  - In the case of external fraud, we would consider that the most relevant information for management purposes is not the 'who' (first party, second party, third party) but the 'how' (type of fraud, channel, product), to ensure the adequacy of risk mitigation and controls. The proposals would have an impact in fraud management frameworks and processes, and could impact historical comparability and analysis.
  - Little or no information currently exists on the classifications "first party fraud", "second party fraud", "third party fraud". Banks will have to look at all existing claims in their risk databases to review the risk description before assigning it to the appropriate category; therefore, clarifications would be very helpful.
  - In External Fraud, the definitions of second and third party fraud are confusing, and their segregation does not provide added value. In the proposed taxonomy, 2nd party fraud are non-cyber, non-data theft events in collusion with another person, and 3rd party fraud are non-cyber, non-data theft events without the knowledge of another person. Fraud risks and controls are set indistinctly to this collusion / non-collusion.
  - Regarding cyber events, not all of them can be considered as External Fraud. For example, certain cyber events such as DDOS or ransomware, would be better classified under BDSF Level 1. Cyber-attacks do not fit neatly into fraud categories as fraud may not be the intent. Also, many cyber events are not linked to an economic loss.
  - Regarding data breaches, if the data breach is caused by a cyber-attack, should it be reported under External Fraud (2.2 or 2.3) or under Clients (4.3)?

- **Clients, Products and Business Practices**:
  - A number of new items in CPBP are a little unclear definitionally. For instance, 4.1 (Client mistreatment / failure to fulfil duties to customers) definition includes the concept of "duties to customer". This term is ambiguous, and more description, details or examples would be needed to fully understand the scope of this category. Would incentive driven poor sales practices be captured here and post-sale related issues? Should the wording in some way reference conduct related issues in the definition? i.e. rather than inappropriate/indelicate behaviour this could refer to conduct."
  - We consider that category 4.3 (Improper market practices, product and service design or licensing) is too wide, and several risks are being mixed (market abuse, product design or not having a license to operate). From our point of view, at least product design should have its

own risk category. Where would providing inaccurate or mis-leading information to clients sit? Maybe sales service failure or potentially product and service design? Could this category also include marketing related issues?

- The scope of category 4.5 (Rights/obligation failures in preparation phase) is not clear. We would need more detail of what this risk encompasses because if it is only related to following the appropriate procedure for handling legal processes, it should be classified under EDPM Level 1. Otherwise, the fact of having failures in contractual obligations is very broad and would overlap with many other risks.
- Similar to the comment included in Internal Fraud, we see category 4.8 (Accidental sanctions violations) as already included in category 4.9 (Accidental money laundering and terrorism financing).
- The new Level 2 "Accidental money laundering and terrorism financing" seems misleading to us as it includes also fines for deficiencies on AML processes but with no occurrence of accidental flows related to AML.
- Level 2 of the risk categories does not always seem to be exhaustive. For example, in the case of a model error, the draft RTS retain the following categories: the "Model methodology design error" and the "Model implementation and use". In banks, all phases of a model's life cycle (Development, Review, Approval, Implementation, Use, Ongoing Management) are considered in the management of risk categories.

- **Damage to Physical Assets**:
  - In Damage to Physical Assets, all events should be included in this category, and not split between Internal Fraud and DPA.
  - Due to the absence of Level 2 in this category, we would like to confirm if existing external events like natural disasters would still be mapped to this category.
  - Further clarification is needed on the pandemic subject: especially whether pandemic topics are included or not in this Level 1 risk..

- **System Failures**:
  - We regret that the operational risk taxonomy as proposed in the drat RTS is not more aligned with the EBA's SREP guidelines. For example, the categories "ICT data integrity", "ICT change", "ICT security risk" are not clearly identifiable in the draft RTS classifications. However, it is a clear request that the ECB has made to certain banks to rely on the EBA's SREP guidelines on this matter.
  - There are IT risks that do not necessarily imply service disruption. For example, failure in asset management can lead to vulnerabilities or obsolescence that does not allow business to evolve
  - "Hardware failure not related to management of transactions": Does this type of business disruption caused by a human error include malicious and non-malicious events? (Example: DDoS is not a fraud). The management of transactions will also need to be well defined."

Inadequate business continuity planning / event management": we don't understand the presence of this line, which is an organisational subject.

- **Execution, Delivery and Process Management**:

  - Risk category 7.2 (Client account mismanagement) overlaps with many other risks, and we would need more specification of its scope. What would be the definition of "Inadequate management"? It could be similar to some risk types in CPBP Level 1.
  - Risk category 7.3 overlaps with 4.5, and this is evident from the definition itself, as 7.3 has the same description as part of 4.5.
  - Regarding 7.5 Improper distribution / marketing, we think this should be included in CPBP Level 1
  - There is a need to clarify what would be classified as 7.9 (Regulatory and Tax authorities including reporting) vs any other regulatory compliance risk. This category appears too broad from a compliance perspective.
  - Third party definition needs to be clarified. Should the industry refer to TPRM concept (entity providing a service) or to something else?
  - We have noticed that purchasing isn't covered by the definition. Would you please explain the rationale?
  - Third party management failures (line 49): We are unable to identify under which level 2 category –the third-party failure, not related to internal third-party monitoring should be linked. Third party management failures may also occur as a result of internal execution, delivery and process failure.
  - Clarification is needed that Data Management category includes general management of data, and not only client, employee, and proprietary data.

In relation to the Attributes proposal, we consider it is a mixture of different concepts, such as risk types, ESG factors, loss type , business line, etc..

We would also raise specific observations in relation to some of the attributes:

  - The rationale for banks being required to differentiate between legal cases that are related to misconduct from those that are not lacks clarity. It's unclear why 'Legal risk – misconduct and other' is added as an additional attribute. Conduct, as a transverse risk, is much broader than Legal Risk, so it seems inappropriate to have an attribute covering misconduct under Legal risk.
  - We would appreciate clarification on the difference between the Market Risk flag and the Trading and Sales flag. Currently, it seems both flags would be checked simultaneously in most or all cases.

- We think that an event classified as 7.4 (Data management) could be linked to the Model Risk attribute, because there can be errors in the design, development, parameter estimation, etc., linked to erroneous data.

It would be helpful to receive clearer definitions and examples around the proposed Level 2 and attributes taxonomy to facilitate a more consistent implementation across institutions. A mapping of the new Level 2 taxonomy with the BCBS Level 2 taxonomy would also be useful.

In the case of Level 2 and the Attributes, the adaptation of banks' processes and systems to the new taxonomy will require, at least, 2 years from the date of entry into force of the RTS for the purpose of recording the new operational risk losses. The reason for this is that the main challenge for firms is to establish the classification process. Because the adaptation is not automatic, it must be performed on event-by-event basis and a lot of manual work is required. Therefore, entities will be required to devote a lot of time and resources. It is also very unlikely that historical risk descriptions contain information to correctly categorize based on new concepts introduced such as intentionality of the loss. Additionally, the level of manual effort required would make it next to impossible to successfully map historic losses to these new risk types.

It is important to note that this effort will be particularly burdensome in the case of large banking groups that will have to implement this new taxonomy in all their subsidiaries, with the cultural change it implies, as well as to cross-regional groups which would face the additional risk and challenge of having to operate more than one regulatory taxonomy. Due to the very detailed classification and heterogeneity of the Level 2 categories, banks will face very serious operational challenges. Indeed, the current processes and risk databases are based on the existing Basel 2 requirements and will need to be revised (including incident databases) to incorporate the more detailed second-level taxonomy of losses, required by the draft RTS; This will require additional resources and efforts given the short timeframe to implement these changes and significant IT developments will be necessary.

Question 2: Do you perceive the attribute 'greenwashing risk' as an operational risk or as a reputational risk event? Please elaborate.

The definition of greenwashing seems too wide to us. Greenwashing is not an Operational Risk per se. It is mainly a factor that could impact the existing risk types, in particular, conduct, litigation, or reputational risks; and in some cases, it could result in operational risk events that must be recognized within the operational risk event base. We consider that this is aligned with the EBA´s Report on greenwashing monitoring and supervision, where it mentions that from the prudential supervisory perspective, several categories of financial risks may be affected by greenwashing, and that it has the potential to create significant reputational and litigation risk.

A greenwashing event is perceived to be an ESG-risk related operational risk event with consequential reputational risk impacts in case an event happens. This follows the understanding that operational risk losses in the form of regulatory enforcement/fines or settlements from civil litigations can arise through greenwashing events. It is considered to be primarily driven by weaknesses in the control environment that do not prevent the reporting and communication of misleading sustainability related information. This can be driven by, for example, ESG-volume reporting processes not adequately set up and controlled, or employees not being sufficiently educated in this topic or even misrepresenting ESG volumes with intent.

Question 3 - Cost of compliance with the reporting requirements: To which Level 1 event types/or Level 2 categories would you map greenwashing losses? Please provide a rationale.

We do not agree with the relation between AML and greenwashing as both risks processes and controls set up are not the same (the possible relation is between both events is a bit premature as of now).

The mapping of greenwashing losses to Level 1 and 2 categories depends on the type of event, and it can be assigned to different categories.

For instance, in the case of Level 1, it could be:

- Category 4 (Clients, Products and Business Practices): it could be classified under regulatory compliance or conduct risk, sales service failure, client mistreatment etc. when a bank markets unintentionally a product as green, when it is not, and is required to make a redress or receives a penalty for it.

-On the other hand, it could also be included under Category 7 (Execution, Delivery and Process Management): if greenwashing arises from an error in the bank's reporting / disclosure activity.

In any case, we broadly agree that greenwashing losses would not be related to Internal Fraud risk type (Category 1), as it is suggested in the table of the EBA taxonomy proposal.

Within the above Level 1, we propose that flexibility should be given in applying the ESG/Greenwashing attributes across all L2 event types within those Level 1.

Finally, we would welcome clear regulatory guidance and confirmation that for L1 event types only events/losses are to be attributed with ESG/Greenwashing, if they relate to an ESG/Sustainability-related process, communication/disclosure or activity.

Question 5 – Which of these attributes do you think would be the most difficult to identify? Please elaborate.

The implementation of the new Level 2 categories and attributes would create very significant challenges for banks. The attributes are a mix of different types of concepts: risk types, loss type, business lines etc. It will require a lot of work from institutions to classify the events to the new taxonomy. Cause analysis and expert judgement are required in many instances, and this will need to be reviewed on a case-by-case basis. We expect the mapping to be largely manual since we do not anticipate the information to be originated from the current source systems.

As an example of possible difficulties in selecting attributes, one could consider the difficulty in identifying whether an extreme weather event is 'normal' or the result of climate/environmental risk change.

The most difficult attributes to identify are :

- Attribute "Credit risk boundary (those not included in RWA on credit risk)" is difficult to identify. We believe that this flag could never be used because each fraud case related to credit risk leads to a default. As each default is considered in the credit risk RWA as per definition, there may not necessarily be any gap.

- Pending losses are temporary and can't be a stable taxonomy element to qualify a risk event. The exercise is theorical as financial institutions have processes and rules dedicated to suspense account

provisioning depending on the materiality and age of the suspense and these processes and rules are the ones which take precedence.

- - Governance risk because such kind of events could show their effects after a significant time, and it could be complicated to trace back the originating cause to poor governance at the time of their occurrence. This includes the difficulties banks encounter to identify governance related events of counterparties that need to be taken into account for ESG risk management.

- Social risk is also very difficult to identify due to the lack of clarity of its scope

In addition, we believe that the attribute "Third party risk" should not be set in case of a "Third party fraud" event. "Third party risk" is always connected to an outsourcing provider, subcontractors of them or supplier.

Overall, the significantly expanded granularity and detail of Level 2 risks and attributes will serve to increase differences in interpretation and implementation across institutions with resulting variations and inconsistencies in risk event classification and reporting.

Question 6: Do you agree with the inclusion of the attribute 'large loss event'? If not, please elaborate.

The attributes "large loss event" and "ten largest loss events" should not be part of the taxonomy as it is not a qualitative attribute and is not stable in time: an incident can be a large loss event during a specific year/window and not during another year/window. Any threshold needs to consider the size of the organisation to be relevant. Even if a loss goes beyond 10% for a specific risk, depending on how low it was previously and the size of the organisation, it can become immaterial.

Besides these attributes need to be supported by dedicated precise instructions as it is the case in the COREP C17.02 or in the Stress Test. Consequently, these two attributes are more reporting related rather than something appropriate for inclusion in a taxonomy.

In addition, it would be burdensome as it would require:

- Recalculation of the average amount to determine if the threshold (10% of the average annual loss calculated over the last 10 years) has been exceeded or not to insert the flag in the corresponding events. The threshold may also be volatile.
- The flag will need to be removed the following year if the event does not meet the threshold any longer.
- Rules need to be defined for the exchange rates to be used for the amounts to be comparable.

More widely, banks will know of their major losses and there will not be the need to flag these separately.

Current regulatory reporting requirements (c17.2) already requests a list of the most relevant new events of the year.

Question 7: Do you think that the granularity of the proposed list of attributes is clear enough? Would you suggest any additional relevant attribute? Please elaborate your rationale?

The attributes are numerous (19 attributes) and their nature seems to be heterogeneous, so it is difficult to identify risk events with common risk characteristics or causes.

- Some of them seem to be reporting attributes (i.e. large loss event, ten large loss events) that can change overtime, others are risk attributes. They should be distinguishable.
- The attributes "Large loss event" and "Ten large loss event" are more financial attributes and make little sense in terms of operational risk. A claim can be one of the 10 largest claims for a given reporting year, but it will be not the following year because some claims are long-lasting. These attributes refer to a notion of reporting and not to a notion of collecting claims in the risk database.
- Some attributes have no mapping to risk categories and therefore, appear to be inconsistent with the other elements of the taxonomy, e.g. "environmental risk – transition risk" attribute.
- Conduct attribute is not consistent with the scope defined for the EBA stress tests by including now events from the 7th category
- It seems to us that the definition of ESG attributes retained in the draft RTS is focused on the ESG risks on banks' counterparties and on the banks' investments whereas according to the CSRD, banks are required to measure the impact of ESG risks on their own activities and the impact of physical climate events on business continuity.
- Some attributes correspond to business lines of the Basel framework, such as retail, commercial banking, trading and sales, other. However, the business line of the Basel framework is a reporting axis for a business that carries a risk and not a risk as such.
- Some attributes are automatically deduced and systematic, therefore without added value to the risk taxonomy (e.g. Model risk, Legal misconduct), and we believe this attribute should be removed.

In relation to specific attributes:

- Legal Misconduct attribute:
    - We disagree with this classification which implies all tax events are conduct issues. It does not make the difference between a "tax evasion event" which could be considered as conduct and an "erroneous tax/regulatory reporting" which is a process execution event. In addition, the definition of the conduct risk events proposed in the matrix is different from the one given in the Stress Test guidelines by including now events from the event type 7. Consequently, this attribute will create inconsistencies between the various reporting sent to the supervisory and regulatory authorities.
    - This taxonomy considers that we are in a case of Legal Misconduct if the event has an impact on the market (mismarking, insider trading) or on the client. In the event of misconduct by an employee, this internal impact is not considered in this taxonomy, which is therefore not aligned with the RTS definition (article 4, paragraph 52a, point (d) of Regulation (EU) 575/2013).

- The "misconduct" approach considers the responsibility of the group and not only the individual responsibility of its employees.
- The Basel event type 2 “Regulatory and Tax authorities, including reporting” is considered a legal misconduct event in the matrix.

- Legal Other than conduct Attribute:
  - The definition of the attribute that should exclude conduct topic includes however the following definition: (f) non-compliance with any requirement derived from contractual arrangements, or with internal rules and codes of conduct established in accordance with national or international rules and practices”. We believe that this attribute should be clarified as to whether conduct events are included or not.
  - It is not clear why AML is a maybe to "Legal risk other than conduct" and Sanctions is a no.

- ICT Attribute
  - The ICT attribute definition refers to security (malicious aspect) and not safety (human error; for instance the use of network and information system). This seems to be restrictive and will be difficult to implement without clarifications.

Not all aspects of misconduct and legal risk should be mapped to internal fraud as an event may give rise to legal risk even if an error was not made intentionally.

Another element of complexity is the relationship of one event to many attributes, which will require care to avoid double or triple counting losses when reporting through multiple flags.

In conclusion, the rationale of the matrix presentation of categories and attributes seems unclear to us and difficult to implement as such. Moreover, depending on whether the mapping of certain risk categories with certain attributes is automatically deduced or not allowed, this will add complexity, create inconsistencies and will not pursue the taxonomy objectives.

While additional attributes can be theorised, the proposal has already put forward 15 new attributes which represent a significant implementation and interpretation hurdle.

Question 8: Would it be disproportionate to also map the three years preceding the entry into force of these Draft RTS To Level 2 categories? If yes, what would be the main challenges?

The Level 1 event types are already challenging given that the new definitions will require the reclassification of certain events from previous years. We therefore consider it disproportionate to require banks to reclassify their historical operational risk losses of their loss data set to the new Level 1.

Requiring banks to, in addition, report the Level 2 categories for the previous three years would be even more disproportionate, particularly in light of the levels of granularity which are much greater than those currently applied and those of other jurisdictions.

The main reason for this is that the adaptation is not automatic, it must be performed on an event by event basis and a lot of manual work is required. We would note that in some cases there is likely to be a lack of information and data available rendering the retrospective mapping unfeasable and unworkable, which has been confirmed by firms' practical experience of seeking to undertake such operations.

Banks will already have to face a significant challenge having to adapt their processes and systems to the new taxonomy for the purpose of recording new operational risk losses. It is important to note that this effort will be particularly burdensome in the case of large banking groups that will have to implement this new taxonomy to all their subsidiaries, with the cultural change it implies.

Question 11: Which of the provisions of Article 317(7), as developed by the draft RTS on the development of the risk taxonomy, and Article 318 of the CRR would be most difficult to implement after a merger or acquisition for the reporting entity? Please elaborate.

The most difficult part is the short timeframe to implement the risk taxonomy after a merger or acquisition of an entity. It will take time to analyze and integrate the database of the acquired entity and build mapping tables and migration rules.

We think that neither the acquiring entity nor the acquired company should be obliged to build a risk taxonomy with retroactive effect or reclassify historical operational risk losses. As previously mentioned, such adaptation would not be automatic and would need to be performed on event-by-event basis with a lot of manual work required. Associated challenges involve the risk of insufficient historical data being available to undertake an accurate classification rendering the exercise not possible. We believe that the effort to build a loss data set should be applicable to operational losses starting from the date of merge or acquisition and at least two years should be allowed for this. The proposed proxy of the EBA proposal will be used for the purposes of calculation of the annual operational risk losses meanwhile.

With regards to Article 2, in case of different currency used by merged or acquired entity from the currency of the acquiring institution, we think that the exchange rate to be used for reporting purposes should be dependent on the instructions for each reporting template. We believe that each entity should be allowed to integrate or record the acquired entity´s data in its database based on its own data model and rules in place for managing events collected in local currencies.

The institutions may manage the data base including operational risk losses in their local currency and, depending on the reporting obligation, use the requested exchange rate (year-end, monthly average, etc.) to convert it into Euros.

Question 12: In your experience, would the provisions of this article apply to most mergers and acquisitions, or would data usually be promptly implemented in the loss data set of the reporting institution?

Article 3 provides for the use of proxies for the calculation of the annual operational risk loss and its distribution per type of loss during the first year in case of a merger or acquisition of another company.

The one-year period to integrate and adjust the losses from merged or acquired entities or activities is too short given the heavy workload required to map historical internal loss data to event type. Depending on the size/materiality of the acquired entity in comparison with the absorbing entity the delay could be

longer/shorter. We consider that a two year period should be allowed for the integration of the data set of the acquired or merged company.

We consider that the use of these proxies will apply to most mergers and acquisitions given that any data base integration will require first the review of the existing data base of the merged or acquired entity, if any, to check its completeness and quality. Any data base of a merged or acquired entity will need to be of sufficient quality to be integrated.

Question 13: Are there other adjustments that should be considered in these draft RTS? If yes, please elaborate.

- The consultation asserts that the Level 1 and Level 2 categories have been designed, "by construction", to be "mutually exclusive and collectively exhaustive". It seems that this objective has resulted in significantly increased risk granularity with similar categories differentiated by non-risk related factors.
- Some level 2 classifications can be misleading. For example, some cyber-attacks resulting in data theft will not be classified as cyber-attacks, but as data theft manipulation. Therefore, the cyber-attacks category would not be complete.
- Model/methodology design error: we should assume that a model is never perfect, making losses due not to an operational risk but to the nature of what a model is.
- In the case of mergers and acquisitions, we can note that operational losses would have occurred under different management and business set-up, and it may therefore not be appropriate to take these forward.
- We wonder about the effective implementation date of the three draft RTS, especially the first reporting date. This RTS, which seems to be limited to historical incidents, impacts in reality the whole operational risk framework (RCSA, controls, …), as taxonomy applies across all components of the framework. If a stock reallocation has to be made on the past 3 years, it will require a detailed analysis, which will be time consuming and excessively burdensome.

AFME Contacts

Mark Bearman
Director, Capital & Risk Management
mark.bearman@afme.eu
+44 (0)20 3828 2675