


POSITION PAPER



ESBG response to the EBA consultation on Draft RTS on establishing a risk taxonomy on operational risk; on the conditions under which it would be unduly burdensome for an institution to calculate the annual operational risk loss; and on the adjustments to an institution's loss data set

ESBG (European Savings and Retail Banking Group)

Rue Marie-Thérèse, 11 - B-1000 Brussels

September 2024



Questions

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.

Although the consultation paper tries to clarify the granularity of and the distinction between the different level 2 categories with regard the current framework, we believe that it is not clear enough.

The lack of clarity comes from the fact that a more granular second level creates a challenge to map the third level event types of the internal taxonomy.

The update of Level 1 definitions represents a change compared to Loss event type classification defined in Article 324 of CRR in Table 3 (e.g. Damage to Physical Assets includes event types which are not used in Level 2 categories, like war, riots, terrorism etc.).

The granularity on second level is too detailed to provide proper mapping from 3 level of event type taxonomies. There is good example of Loss event taxonomy for the granularity on second level defined in international standards set out in the Basel taxonomy (<https://www.bis.org/publ/bcbs128.pdf>), with examples on level 3.

In most of the cases the banks consider both first party and third-party frauds in case of loans in credit risk RWA, hence removing credit related operational risk events from the internal loss data has withdrawing impact on risk management. Further on, first party frauds are not event types but classification attributes to identify in which stage of the lifecycle the fraudulent activity occurred as such could be used as flags for the fraud events. Concise first and third party fraud definitions can be found in EBA/CP/2014/08 (europa.eu). In addition, it is not clear what is meant with second party fraud.

Against this backdrop, the new proposed taxonomy will have many implications for the management of operational risk of entities.

Rational:

The taxonomy of operational risks is the basis on which the operational risk framework is built since this risk includes different risks of different nature and require differential management by entities. Therefore, it is necessary to have a clear and concise taxonomy of risks at all levels that allows entities to record losses in a homogeneous and uninterpretable way. Providing clarity in the taxonomy will also allow assigning different roles and responsibilities in management and control functions that will avoid disruptions and lack of action in each type of risk.

The regulatory categories were established almost 20 years ago (BIS II), with much of the industry having changed since then. Many risks have become independent and new risks have emerged, as a consequence of their own evolution



or supervisory priorities. There could even be some overlap between regulatory categories, with entities having mapped, in terms of management, such overlaps to their own risks that are generated in the internal taxonomy. It is true that several of the regulatory categories are very broad or there are certain overlaps between them (business practices, conduct and legal...) but there is no univocal mapping framework, which makes the exercise difficult. We believe that work should be done to avoid the possible disconnection between regulatory reporting and banks' risk management criteria and taxonomies, which would increase the difficulty of explaining operational risk exposures and losses to supervisors.

The regulatory categories are the basis for regulatory exercises (e.g. stress-test) and for comparability exercises between entities by the supervisor, while entities use their internal risk management taxonomy to establish action plans, it is the basis for the management of the levers or drivers (self-assessment, scenarios, KRIs, loss forecast). Therefore, entities have their own "internal mappings" between the regulatory categories and their internal categories, which are different between entities. Consequently, in large entities there are categorizations with ORX taxonomies and then more granular disaggregation, which change by entity. Any modification will affect the history and it will be necessary to modify 5 years for regulatory years, which is not easy and could cause heterogeneity in the mappings, greater difficulty for comparability, complex developments, etc. On many occasions, entities come from mergers and acquisitions, with less origin information, and historical mapping can involve very significant efforts and implementation difficulties.

The operational risk management pivots on each entity's corporate risk catalogue, on which the three lines of defense are structured and on which work is being done to advance, use of common risk language, culture, etc. Much progress has even been made in granular reporting for the senior management, who regularly receives information on the risks of the corporate taxonomy. The establishment of new regulatory taxonomies that continue to pivot on the 7 level I categories, if they are not used in management, could not help to improve the management of entities and produce very different mappings by the entities. Therefore, the new level II, to the extent that it does not map correctly with the current level II, will generate mapping problems in the history, developments in the entities' systems and will not help in risk management and culture.

The challenge is to generate better information and provide common language in organisations to share risk information where it is spoken and managed with the same understanding.

Therefore, in our opinion, it is a priority to improve the relationship between the regulatory taxonomy and the risk taxonomy in the management of entities. To do this, it must be taken into account the way the entities are managed, since this management is carried out on corporate risks (human and technical resources assigned, which will continue to grow in future years).



As indicated, we believe that it is essential to first homogenise risk definitions, including opinions from the industry that allow the process to have more consistency before addressing the opening of risks. It could cause considerable complexity that would imply developments in the event of not carrying out the previous exercise of homogenisation of definitions. There must be a clear and unique definition of new risks before changing the taxonomy to avoid different interpretations by entities, homogenising risk definitions, understanding origins and causes and adapting to current reality:

- Exclusions
- Possibility of non-exclusive risks (event with multi-assignment of risks due to external fraud and outsourcing, for instance, or with internal fraud). This has important implications for databases because there may not be enough flags that can be set to include attributes. This is a very relevant issue in the database management process (multiple causes managed as a single event). The use of flags could help, but it also makes their implementation difficult in automatic feeding processes that involve developments and resources. It is necessary to seek balance in the use of flags. There needs to be a constructive debate with the industry about when flags should be included in events, to see if there should be a flag or a risk categorisation. In some cases, flags would be difficult to determine or implement. Including in the operational risk database some of the brands proposed in the EBA draft document is complex and we believe that there should be a prior debate between the industry and the regulator. Throughout the draft document some attributes that are difficult to identify are detailed.
- Flags or attributes are necessary in case of factors that are not considered as types of risks (for example, climate issues) and also when the same type of event can be categorized into more than one type of risk (for example outsourcing in an event of external fraud), but in some cases it will be very difficult to implement, so a balance must be sought between the need for a flag and the difficulty of implementation (e.g governance or greenwashing flag).
- Flags could facilitate the interaction between the person responsible for the management and control of the different types of risks that are interconnected, but their maintenance and correct use will require time and resources to be used, so they must be balanced for appropriate use of time and resources.

The new risk taxonomy that is developed in this EBA draft RTS with 7 Level 1 Risks and 38 Level 2 categories should be much more detailed with regard to the new Level 2 categories that are proposed, contributing in each case a **clear and concise description that allows entities to classify clearly and without interpretation the loss events recorded in the database**, providing examples of specific situations that, if they occurred, would give rise to loss events classified in each of the 38 categories proposals.



Observations on specific risks of the proposed new taxonomy:

- Legal Risk:

Legal Risk is a Level 1 risk in credit institutions' corporate risk category and all the operational risk management levers, and the three lines of defense model are articulated through this internal category, and therefore, considering the legal risk as Level 1.

Considering legal risk as an attribute (legal risk – Misconduct/legal risk – Other than misconduct) will mean an even greater separation between regulatory reporting and the risk management criteria and taxonomy of the entity, which is not an improvement in the management of entities and will make it increasingly difficult to explain exposure to operational risk and losses to the supervisor.

With this scheme, there are potential operational legal risk events that are not covered by the proposed risk categories, such as possible sanctions derived from legal non-compliance not related to inappropriate conduct. According to the EBA draft RTS, these cases would be classified in reference 7.9 [Execution, Delivery & Process Management Level 2 classification/Regulatory and Tax authorities, including reporting], which represents an important difference in criteria with respect to the entities' corporate risk category, which would classify it at level 1 of legal risk.

The creation of a specific flag in the database to mark the attribute (legal risk – Misconduct/legal risk – Other than misconduct) implies a development in systems that will entail greater costs in economic and personnel resources, for the adaptation of the new approach to risks, which will not correspond to an improvement in operational risk management.

- Model Risk:

The model risk attribute does not provide any value since the model risk is included in the risk taxonomy of the categories indicated below and it is mandatory that all losses that are in those categories have that attribute:

- Level 1 (Execution, Delivery & Process Management) and Level 2 (Model implementation and use).
- Level 1 (Clients, Products & Business Practices) and Level 2 (Model / methodology design error).

Therefore, by having a “yes” attribute in these categories, all events registered in these risks will have the model risk attribute, which does not make sense. If only a part of the losses from these risks were model risk, the flag to be registered would have to be manually set by the user, which would not make sense either. **We propose to remove the attribute.**



- Cyber:

Cybersecurity losses are classified into two levels of Risk Level 1 and corresponding Level 2 categories:

- External Fraud: losses due to cyber-attack with or without data theft/manipulation.
- IT failures: cybersecurity losses not related to third-party attacks.

Separating cybersecurity losses into these two risk levels will be difficult, as it is no longer always possible to determine the losses that come from a system failure from those that are generated by a cyber-attack. This fact will also make comparability between entities difficult.

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

We perceive the attribute “greenwashing risk” as an operational risk event but with a component of reputational and/or conduct risk, similarly to all operational risk events. It is operational risk as long as sanctions can be imposed. In addition, “greenwashing risk” also includes possible lawsuits and claims from clients against the entity.

Therefore, it is necessary for the EBA to clearly and accurately define what is considered greenwashing and what is considered transitional environmental risk. If a green requirement is not met, the associated operational losses should be marked with one attribute or another. Along these lines, if a sanction is received for social and/or governance issues, the resulting losses should be marked as ‘social or governance’ or transition risk, not both.

Lastly, considering the previous points, whereby risks would be ESG-related or related to conduct, legal and other relevant fields, ESBG believes that it should be called “greenwashing case”.

Question 3: To which Level 1 event types and/or Level 2 categories would you map greenwashing losses? Please provide a rationale.

Greenwashing losses could be mapped to Level 1 event type “Clients, Products & Business Practices” and Level 2 category “Improper market practices, product and service design or licensing”, according to the own definition provided in the consultation paper that refers to (i) “(...) *all types of market abuse and manipulation*” -given that manipulation can be understood as selling something as green when it is really not green-, and (ii) “(...) *the design of a product/service does not meet client’s needs*” -given that client’s need in terms of sustainability would not be satisfied-, as well as “Client mistreatment/failure to fulfil duties to customer”, “Rights/obligation failures in preparation phase”, “Sale service failure” and to Level 1 event type “Execution, Delivery & Process Management” and Level 2 categories “Rights/obligation failures in execution phase”, “Improper



distribution/marketing” and “Regulatory and Tax authorities, including reporting”.

Greenwashing can occur when financial institutions fail to properly disclose information about the environmental impact of their products or services, or when they make unsubstantiated claims about their environmental benefits and are not transparent, consistent, and reliable of environmental information and disclosures.

In addition, greenwashing losses could also be mapped in the following categories:

- Clients, Products & Business Practices (Level 1):
 - o Client mistreatment / failure to fulfil duties to customer
 - o Rights/obligations failures in preparation phase
 - o Sale service failure

Rational: losses due to supervisory sanctions and/or lawsuits and claims from clients due to inadequate product design and marketing, for instance, by having advertised and/or sold a financial product as green, when it really was not.

- Execution, Delivery & Process Management (Level 1):
 - o Rights/obligations failures in execution phase
 - o Data management
 - o Improper distribution/marketing
 - o Regulatory and Tax authorities, including reporting

Rational: losses due to supervisory sanctions and/or lawsuits and claims from clients due to the inadequate design and marketing of products, such as green financial products when they really were not. The bad practice is due to an error in process execution/management.

Also, we propose eliminating the link of greenwashing risk with the following Level 2 categories because we do not see the relationship:

- Internal Fraud (Level 1):
 - o Intentional sanctions violation
 - o Intentional money laundering and terrorism financing
- Clients, Products & Business Practices (Level 1):
 - o Accidental sanctions violations
 - o Accidental money laundering and terrorism financing



Question 4: Is “Environmental – transition risk” an operational risk event? If yes, to which Level 2 categories should it be mapped? Please provide a rationale.

ESBG understands that “Environmental – transition risk” is a risk driver and not an operational risk event proper. This is due to the fact that it is a non-financial risk that crosses different operational sub-risk types and can result in operational risk event materializing under the specific operational sub-risk type. The following drivers can be highlighted:

- Regulatory requirements (e.g. sustainability certificates, disclosures) can trigger policy changes causing ESG misconduct cases in the past, misrepresent sustainability-related practices or the sustainability-related features of its investment products, non-adherence to or missing internal ESG risk management rules and non-adherence to voluntary or mandatory climate and environmental reporting events (governance risk).
- Behavioral changes of consumers, suppliers, employees, and investors can cause loss event due to failures in adaption of the ESG strategy and related business practices or by not pursuing the strategic opportunities and addressing the risk proactively from transition towards climate-neutral economy (social risk).
- Behavioral changes of consumers, suppliers, employees, and investors causing loss event due to failure in strategy to address, measure and support sustainable transition, publicly controversial financing or activity due to preference changes and missed expectation to provide more sustainable products and services (social risk).
- Technical developments can cause misconduct by a new technology or digitalization (e.g. fundamental right violation, product not meeting the needs of people with disabilities etc.) (social risk). Technical developments can cause if it is not sustainable (e.g. AI with high energy need) (environmental risk-transition risk).

They all fall into other risks (governance, social etc.).

However, “Environmental – transition risk” could be treated as a “greenwashing” operational risk event as long as sanctions could be imposed.

Given that it is not clear at the current stage, we would propose to map it to Level 1 event type “Execution, Delivery & Process Management” and Level 2 category “Regulatory and Tax authorities, including reporting”. Additionally, ESBG considers that the EBA should define clearly and accurately what is considered transitional environmental risk and what is social risk and governance risk so that there are no interpretations and entities can classify their losses following homogeneous criteria.

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

We think that the following attributes are the most difficult to identify:

- **Pending Loss:** is a loss type, similarly to uncollected revenues, provisions and timing loss, and it should not be an attribute.
- **Large loss event:** IT development is required to generate the flag at the event level in the database. Identification will entail an economic cost for the entity and may affect the performance of the database, by having to calculate the value of “large loss event” each time a new loss event is recorded. However, this information could be reported to the supervisor with the periodicity deemed appropriate. We propose to eliminate this attribute for the registration of loss events in the database.
- **Legal risk – Misconduct:** for Level 2 categories that are not automatically assigned with this attribute (blank field), a manual event-by-event identification is required to identify whether the attribute should be assigned or not, which makes impossible the automation of the flag in the database.
- **Legal risk – Other than misconduct:** for Level 2 categories that are not automatically assigned with this attribute (blank field), a manual event-by-event identification is required to identify whether the attribute should be assigned or not, which makes impossible the automation of the flag in the database.
 - o To note, a clear distinction between legal risk- misconduct / other than conduct could eventually create grey areas (e.g. Data privacy breach / confidentiality mismanagement as solely “other than misconduct”).
- **Model risk:** it is proposed to eliminate this attribute because its identification does not contribute anything, since there are two level 2 risk categories that have this attribute automatically assigned (field with ‘yes’). It could therefore be seen as redundant.
- **ICT risk:** for Level 2 categories that are not automatically assigned with this attribute (blank field), a manual event-by-event identification is required to identify whether the attribute should be assigned or not, which makes impossible the automation of the flag in the database. On this note, ESG would like to enquire with the EBA whether the expectation is to perform a root cause analysis to identify ICT related causes.
- **Third party:** for Level 2 categories that are not automatically assigned with this attribute (blank field), a manual event-by-event identification is required to identify whether the attribute should be assigned or not, which makes impossible the automation of the flag in the database.
- **Environmental risk-physical risk:** for Level 2 categories that do not correspond to the risk of Damage to physical assets, manual event-by-event identification is required to identify whether the attribute should be assigned or not, which makes impossible the automation of the flag in the database.



- **Social risk:** manual event-by-event identification is required to identify whether the attribute should be assigned or not, which makes impossible the automation of the flag in the database.
- **Governance risk:** manual event-by-event identification is required to identify whether the attribute should be assigned or not, which makes impossible the automation of the flag in the database.
- **Greenwashing risk:** manual event-by-event identification is required to identify whether the attribute should be assigned or not, which makes impossible the automation of the flag in the database.

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

We do not agree with the inclusion of the attribute “Large loss event”. It does not make much sense, considering that it will be redundant with existing reporting requirements, i.e. internal reporting requirements for the supervisor request to inform about level 1 categories (template C17.1 – OPR details 1).

Moreover, “Ten largest loss events” also seem unnecessary, as it also represents an additional and moving reporting burden, as it would lead to unnecessary IT investments.

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

According to our view, the list of attributes proposed is too exhaustive and the preset constellation is not necessary, as these would require entities to collect “descriptive information about the drivers or causes of the loss events”, that is, much more granular and particular information at the event level for registration in the database, which makes automatic identification difficult of each case.

The level of detail of any descriptive information shall be commensurate with the size of the gross loss amount. The flags can be used to support a structured root cause analysis so it would be imperative to define proper set of flags.

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?

Yes, we believe that mapping the three years preceding the entry into force of the Draft RTS would be disproportionate. It would be a huge burden for credit institutions to report events from the last three years with the new Level 2 categories. The current granularity level is too low, which makes it difficult to map events which are not included on second level.



It goes from the current 21 categories to 38, which means that an event-by-event analysis would have to be carried out to determine the new Level 2 category to be assigned (being also possible to map between several categories of the new ones). On the other hand, it should be noted that, in general, in the reports that are currently made to the regulator, they are not being lowered to Level 2, so there is no need to have to do it now retroactively and more so without a transitional period.

In addition, we believe that it is especially difficult if there is a considerable volume of events originating from integrated entities.

Question 9: Is the length of the waivers (three years and one year) for institutions that, post merger or acquisition fall into the EUR 750 million – EUR 1 billion band for the business indicator, sufficient to set up the calculation of the operational risk loss following a merger or acquisition? If not, please provide a rationale.

Yes

Question 10: Are there other cases where it should be considered to be unduly burdensome for institutions to calculate the annual operational risk loss?

For instance, when the business indicator of an institution exceeds EUR 1 billion and the merged/acquired institution cannot provide good data quality.

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.

According to our view, in a merger/acquisition process the most complicated thing to implement would be the calculation of the operational losses of the integrated company, as established in Article 318 of the CRR, mainly due to possible limitations in the quality of information available in the integrated institution database.



The granularity of losses feeding the loss calculation, based on the merged / acquired institution level of available details in loss collection and classification.

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?

Both cases are equally possible.

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

In our opinion, it is necessary for the EBA to clearly and accurately define what is considered transition environmental risk, and what is greenwashing risk, social risk and governance risk so that there are no interpretations and entities can classify their losses following homogeneous criteria.



About ESBG (European Savings and Retail Banking Group)

ESBG is an association that represents the locally focused European banking sector, helping savings and retail banks in 17 European countries strengthen their unique approach that focuses on providing service to local communities and boosting SMEs. An advocate for a proportionate approach to banking rules, ESBG unites at EU level some 871 banks, which together employ 610,000 people driven to innovate at 41,000 outlets. ESBG members have total assets of €6.38 trillion, provide €3.6 trillion loans to non-banks, and serve 163 million Europeans seeking retail banking services.

Our transparency ID is 8765978796-80.



European Savings and Retail Banking Group – aisbl
Rue Marie-Thérèse, 11 ■ B-1000 Brussels ■ Tel: +32 2 211 11 11 ■ Fax : +32 2 211 11 99
Info@wsbi-esbg.org ■ www.wsbi-esbg.org

Published by ESBG. May 2024