EBA/RTS/2025/03

04 August 2025

Final Report

Draft regulatory technical standards on

— 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 under Article 317(9) of Regulation (EU) 575/2013;
— specifying the condition of 'unduly burdensome' for the calculation of the annual operational risk loss under Article 316(3) of Regulation (EU) 575/2013;
— specifying how institutions shall determine the adjustments to their loss data set following the inclusion of losses from merged or acquired entities or activities under Article 321(2) of Regulation (EU) 575/2013.

Contents

1. Executive summary

The CRR 3 includes amendments to the operational risk area, where a revised framework is introduced and all previously existing approaches for the calculation of the regulatory capital are replaced by the business indicator component (BIC). The BIC is based on the business indicator (BI), which measures an institution's volume of business.

While the loss component in the Basel framework is set to 1 in the context of the European implementation, attention is still given to how the operational risk losses are calculated and stored in the data sets. In particular, in order to calculate the annual operational risk loss, institutions with a BI above EUR 750 million need to build and maintain a loss data set that includes losses above a certain threshold, in the ten-year time window.

Subsequently, the EBA has received several mandates concerning the data collection and governance of the loss data set. This draft Consultation Paper (CP) deals with three of these mandates:

1) A draft regulatory technical standard (RTS) on 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 under Article 317(9) of Regulation (EU) 575/2013;

2) A draft regulatory technical standard (RTS) on specifying the condition of 'unduly burdensome' for the calculation of the annual operational risk loss under Article 316(3) of Regulation (EU) 575/2013;

3) A draft regulatory technical standard (RTS) on specifying how institutions shall determine the adjustments to their loss data set following the inclusion of losses from merged or acquired entities or activities as referred to in Article 321(1) of the CRR under Article 321(2) of Regulation (EU) 575/2013.

Regarding the first mandate, the draft RTS establish a risk taxonomy that includes Level 1 event types in line with those envisaged in the CRR2, Level 2 categories that specify in greater detail the corresponding event types, and a list of attributes that increase the flexibility of the framework and the level of information available to supervisors. By construction, Level 1 event types and Level 2 categories are mutually exclusive and collectively exhaustive, while multiple attributes can be assigned to a single loss event.

As far as the second mandate is concerned, the CRR 3 allows the competent authority to grant a derogation to an institution whose BI is between EUR 750 million – EUR 1 billion, when the institution proves that such calculation would be unduly burdensome. The draft RTS specify that the calculation of the annual operational risk loss should be deemed as unduly burdensome, for up to three years, when an institution has a BI higher than EUR 750 million following an operation of merger and acquisition. In addition, also for institutions whose BI temporarily passes EUR 750 million should be waived from the calculation of the annual operational risk loss. Finally, bridge institutions set up according to Article 40 of the BRRD should be also waived from this requirement.

Finally, regarding the third mandate, the draft RTS require institutions that are subject to an operation of merger or acquisition, or that acquire an activity, to incorporate the loss data set of the acquired or merged entity, or activity, in the currency of the reporting institutions. Furthermore, the loss data set of the acquired or merged entity, or activity, should be incorporated reflecting the risk taxonomy used by the reporting institution. Finally, the draft RTS provide a formula to calculate on a temporary basis, the annual operational risk loss when the institution is not able to include the loss data set of the acquired or merged entity, or activity, into the loss data set of the reporting institution.

The three draft RTS were subject to a public consultation from 6 June to 6 September 2024. Nineteen responses were received, of which fourteen were published on the EBA website. The EBA also hosted a workshop with industry participants on 12 November 2024. The three RTS have been amended to accommodate most of the comments received by stakeholders.

Next steps

The draft regulatory technical standards will be submitted to the Commission for endorsement following which they will be subject to scrutiny by the European Parliament and the Council before being published in the *Official Journal of the European Union*.

2. Background and rationale

2.1 Introduction

1. The banking package that implements the Basel III framework in the EU envisages several amendments to the Capital Requirements Regulation (CRR). This includes the introduction in the EU of a revised framework for own funds requirements for operational risk, consisting of replacing all existing approaches for the calculation of the regulatory capital with a single, non-model-based approach: the business indicator component (BIC).

2. Furthermore, the CRR requires institutions with a business indicator (BI) equal to or higher than EUR 750 million to identify and record losses to calculate the annual operational risk loss according to Article 316 of the CRR. Recorded losses contribute to build the loss data set according to Article 317 of the CRR. In order to build a comparable and consistent loss data set, institutions need to assign a loss event to a specific entry according to a risk taxonomy. Article 317(9) of the CRR grants the EBA a mandate concerning the establishment of the risk taxonomy to be used by all institutions when recording losses.

3. To avoid disproportionate efforts from institutions to calculate the annual operational risk loss, an institution whose BI is between EUR 750 million and EUR 1 billion may ask its competent authority an exemption from the calculation of this annual operational risk loss. When granting this exemption, the competent authority should assess whether the calculation of the annual operational risk loss would be unduly burdensome for the institution. Article 316(3) of the CRR grants the EBA a mandate to specify the condition of 'unduly burdensome' for the calculation of the annual operational risk loss.

4. Institutions that perform mergers or acquisitions, or that include activities, should include losses stemming from merged or acquired entities or activities in their loss data set going back 10 years, as soon as the business indicator items related to those entities or activities are included in the institution's business indicator. Since the loss data set of the merging or acquiring entities or activities may need adjustments in order to be merged in a single loss data set, Article 321(2) of the CRR grants the EBA a mandate to provide guidance on how to adjust the loss data set of the merged or acquired entities or activities. Furthermore, the draft RTS under this mandate also provide an alternative calculation methodology when the adjustments to the loss data set cannot be performed promptly.

5. During the three-month public consultation phase that ended on 6 September 2024, the respondents provided a significant number of comments, mostly on the draft RTS for establishing a risk taxonomy for operational risk. In addition, the EBA held an industry workshop on 12 November 2024, where further comments were received.

6. The next sub-sections provide further details on the development of the draft RTS under Articles 317(9), 316(3) and 321(2) of the CRR.

2.2 Draft regulatory technical standards for 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 under Article 317(9) of the CRR

7. According to Article 316(1) of the CRR, institutions with a business indicator equal to or exceeding EUR 750 million shall calculate their annual operational risk loss according to the formula:

$$OR\_loss = \sum_i net\_loss_i$$

where net_loss_i≥ EUR 20 000 (Article 319(1) of the CRR) or EUR 100 000 (Article 318(2) of the CRR).

8. Furthermore, in line with Article 317(7) of the CRR, institutions shall be able to map their historical internal loss data to event type at the request of the competent authority.

9. The EBA is mandated, under Article 317(9) of the CRR, to develop a risk taxonomy that complies with international standards and a methodology to classify the loss events included in the loss data set based on that risk taxonomy for operational risk. This risk taxonomy is central to ensuring data consistency within an institution, as well as comparability across the banking sector.

2.2.1 The structure of the risk taxonomy: Level 1 event types and Level 2 categories

10. While the Basel Committee on Banking Supervision (BCBS) has delivered a new methodology for the calculation of capital requirements for operational risk, it has not updated its risk taxonomy previously used in the Basel 2 framework, which is also used in the context of the CRR 2 framework.

11. Against this background, the EBA made a deliberate choice to develop a risk taxonomy in continuity with the framework of the CRR 2, with the aim of maintaining alignment with the current practice of most institutions. This taxonomy is built on Level 1 event types and Level 2 categories, which retain their quality of being mutually exclusive and collectively exhaustive (MECE).

12. In particular, Level 1 event types describe, in line with international standards set out in the Basel taxonomy[1], the operational risk losses and map them in seven event types that encompass all possible records, without envisaging a residual category. Each Level 1 event type is assigned with specific Level 2 categories that describe in greater detail the corresponding Level 1 event type.

[1] https://www.bis.org/publ/bcbs128.pdf

13. More specifically, the Level 2 categorisation is built through a two-step procedure, which also included an analysis of the Basel Level 2 and Level 3 taxonomy, and the EBA response to the call for advice for the adoption of Basel 3[2]. In the first step, a review of Level 2 categories used by most industry participants was performed. The Level 2 categories that were mapped to only one event type were directly considered as Level 2 categories of the event type they are mapped to. Level 2 categories that were mapped to more than one event type were split into sub-categories that correspond to only one event type with a view to these categories being MECE. Finally, these latter sub-categories were also considered as Level 2 categories of the event type they are mapped to.

14. In the second step, the categories resulting from the first step were adjusted as follows:

- Taking into account historical data, most categories under the same event type were aggregated to ensure that the resulting categories were material enough in terms of either share of loss events or share of loss amounts. Some less-material categories were kept for their strategical relevance or when there was an expectation that future losses will exceed those observed in the past;
- The Level 2 categories used by the industry that were not mapped to any event type, were mapped to the most appropriate category to ensure that resulting categories are collectively exhaustive of all BCBS event types;
- Some Level 2 categories for which the mapping used by the industry was not considered consistent, were mapped to a different event type.

15. As result of these steps taken to develop the risk taxonomy, seven Level 1 event types and 26 Level 2 categories were defined.

16. The following table shows the mapping of the draft RTS with the BCBS operational risk taxonomy (it should be noted that the loss events assigned to the attribute 'third party' – last row of the table – should also be assigned to the relevant Level 2 category of the final draft RTS, on the basis of the underlying type of event).

[2] https://www.eba.europa.eu/finalised-basel-iii-standards-dec-2017-call-advice

Draft RTS Level 1 event types	Draft RTS Level 2 categories	Basel Level 2	Basel Level 1
Internal Fraud	Bribery and Corruption	Theft and fraud	Internal Fraud
Internal Fraud	Internal fraud committed against the institution *(including improper market practices and financial crime classified as internal fraud, e.g. insider trading)*	Theft and fraud	Internal Fraud
		Unauthorised activity	
Internal Fraud	Internal fraud committed against other stakeholders *(including improper market practices and financial crime classified as internal fraud)*	Theft and fraud	Internal Fraud
		Unauthorised activity	
External Fraud	Fraud committed by institution's clients	Theft and fraud	External Fraud
External Fraud	Fraud not committed by institution's clients	Theft and fraud	External Fraud
External Fraud	Data theft and manipulation	System security	External Fraud
External Fraud	Robbery, Burglary and physical theft	Theft and fraud	External Fraud
Employment Practices and Workplace Safety	Inadequate Employment practice	Employee relations	Employment Practices and Workplace Safety
		Diversity and discrimination	Employment Practices and Workplace Safety
Employment Practices and Workplace Safety	Inadequate workplace safety	Safe environment	Employment Practices and Workplace Safety
Clients, Products & Business Practices	Client mistreatment / failure to fulfil duties to customer	Suitability, Disclosure & Fiduciary	Clients, Products & Business Practices
		Selection, Sponsorship & Exposure	
Clients, Products & Business Practices	Data privacy breach / confidentiality mismanagement	Suitability, Disclosure & Fiduciary	Clients, Products & Business Practices
Clients, Products & Business Practices	Improper market practices, antitrust/anti competition *(excluding those events classified as internal fraud)*	Improper Business or Market Practices	Clients, Products & Business Practices
Clients, Products & Business Practices	Improper distribution marketing, including sale service failure	Suitability, Disclosure & Fiduciary	Clients, Products & Business Practices
		Selection, Sponsorship & Exposure	
		Advisory Activities	
Clients, Products & Business Practices	Financial Crime *(excluding those events classified as internal fraud)*	Improper Business or Market Practices	Clients, Products & Business Practices
Clients, Products & Business Practices	Breaches of statute and regulations, other than those specifically assigned to other event types or categories	Improper Business or Market Practices	Clients, Products & Business Practices
Clients, Products & Business Practices	Improper product or service design	Product flaws	Clients, Products & Business Practices
Clients, Products & Business Practices	Model methodology	Product flaws	Clients, Products & Business Practices
Damage to Physical Assets	Natural Disasters	Disasters and other events	Damage to Physical Assets
Damage to Physical Assets	Other external events	Disasters and other events	Damage to Physical Assets
Business Disruption and System Failures	Infrastructure and System failure	Systems	Business Disruption and System Failures
Business Disruption and System Failures	Business Disruption	Systems	Business Disruption and System Failures
Execution, Delivery & Process Management	Processing / execution failures	Transaction Capture, Execution & Maintenance	Execution, Delivery & Process Management
		Trade Counterparties	Execution, Delivery & Process Management
Execution, Delivery & Process Management	Client account mismanagement	Customer Intake and Documentation	Execution, Delivery & Process Management
		Customer/Client account management	Execution, Delivery & Process Management
Execution, Delivery & Process Management	Rights/obligation failures	Monitoring and Reporting	Execution, Delivery & Process Management
Execution, Delivery & Process Management	Data management	Transaction Capture, Execution & Maintenance	Execution, Delivery & Process Management
Execution, Delivery & Process Management	Model implementation and use	Transaction Capture, Execution & Maintenance	Execution, Delivery & Process Management
Attribute third Party		Vendors & Supplies	Execution, Delivery & Process

2.2.2 The structure of the risk taxonomy: rationale for the approach adopted on attributes

17. In line with the industry best practices, these draft RTS complement the operational risk taxonomy with the use of the attributes, also called 'flags'. The use of attributes has become lately an important dimension used in the industry to identify phenomena which cannot be easily captured through the event type dimension.

18. Indeed, the flag is an additional attribute that allows to specify, when relevant, a macro category that is independent from the Level 1 event type classification. The main goal of attributes is to identify risk events with common risk characteristics or causes.

19. The attributes do not have to be mutually exclusive or collectively exhaustive, meaning that specific losses might be flagged several times while others might not be flagged at all: attributes are not supposed to cover all risk events, so specific flags were identified considering which macro categories and sub-aggregation would be most useful from a supervisory perspective.

20. Among the attributes introduced in these draft RTS, some are dedicated to the business lines: to avoid the introduction of additional, not harmonised, definitions for the business areas, these draft RTS rely on the CRR definitions criteria for the Retail, Trading and Sales businesses, with all the other business lines aggregated under 'Other Business Lines', and credit institutions should use at least one attribute dedicated to the business lines for each loss event.

2.2.3 Rationale for ESG attributes

21. Among the attributes introduced in these draft RTS, two are dedicated to ESG: one is aimed at marking greenwashing risk, while the other encompasses the three ESG factors (i.e. environmental – including those related to physical and transition risk – social and governance factors). At this stage, it is deemed important to keep the framework simple, thus the use of two attributes seems fit for the purposes of the taxonomy. However, institutions may decide to use more granular flags if they consider this necessary for their risk management processes.

22. The ESG risk attribute builds on the definition of ESG risks, as introduced in the CRR 3, stating that ESG risk is the '*risk of losses arising from any negative financial impact on the institution stemming from the current or prospective impacts of ESG factors on the institution's counterparties or invested assets*'.

23. The specific nature of ESG risks requires that institutions build appropriate risk management processes allowing the identification, measurement, monitoring and management of these risks. ESG factors manifest their impact through traditional categories of risk, including operational risk. It is expected that the effects of ESG factors will intensify in the coming years, given the forward-looking nature of these risks. Therefore, there is a need to monitor the impacts of ESG factors on operational risk events and losses, in order to be able to identify the trends, potential areas of vulnerabilities, and to take appropriate mitigating actions.

24. For the above reasons, the recommendation for institutions to '*identify whether environmental and social factors constitute triggers of operational risk losses in addition to the existing operational risk taxonomy'* has already been put forward in the EBA Report on environmental and social risks in the prudential framework (EBA/REP/2023/34). This recommendation is now reflected directly in the taxonomy. Harmonised rules for monitoring the impacts of ESG factors on operational risk will allow also monitoring of this risk at the system-wide level.

25. Furthermore, in accordance with Article 430(1), point (h), the CRR 3 widens the supervisory reporting requirements of institutions to include exposures to ESG risks. In this regard, the EBA shall develop draft implementing technical standards (ITS) for the new reporting requirements, providing the competent authorities with the data they need to perform their supervisory activities, including assessing the effect of ESG risks on the traditional risk categories, incl. operational risks. The inclusion of an ESG risk attribute in the loss taxonomy is therefore the first step to identifying the part of operational risk that is linked to ESG factors. In the next steps, the EBA will develop supervisory reporting requirements with a view to developing more accurate ESG risk assessments and ensuring that prudential capital requirements remain appropriately calibrated over time. For that purpose, the collection of relevant and reliable information on ESG risks and their impact on financial losses of institutions is crucial.

26. Next to the ESG risk attribute, the greenwashing risk attribute is isolated due to its specific nature, which manifests itself in different ways than other ESG factors. According to the high-level understanding of the three ESA's[3], greenwashing risk can be defined as losses from practices whereby sustainability-related statements, declarations, actions, or communications do not clearly and fairly reflect the underlying sustainability profile of an entity, a financial product, or financial services. This practice may be misleading to consumers, investors, or other market participants. The impacts of greenwashing risk are therefore not linked to external factors affecting the counterparties or the assets of the institution, but they are linked to specific actions, or lack thereof, of the institution. Typically, the operational losses linked to greenwashing risk would be accrued through litigation processes or penalties imposed by relevant authorities.

27. As the EBA Report on greenwashing monitoring and supervision (EBA/REP/2024/09) revealed, there is evidence of constantly growing numbers of alleged greenwashing cases over the last years. Hence, there is a need to closely monitor this phenomenon in order to be able to design appropriate risk management and supervisory solutions. It will be therefore necessary to collect information on operational losses triggered by greenwashing risks, whereas cases of greenwashing must be clearly separable from other types of misconduct.

28. Since the definitions of ESG risk and greenwashing risk are different in nature, a merge of the attribute for greenwashing risk with the attribute for ESG risks is not considered meaningful. While ESG risks are related to third party and/or invested assets of an institution, greenwashing is an event, such as misconduct or mis-selling, which is directly related to the institution and its actions.

29. While the taxonomy does not prescribe which event types may attract the ESG or greenwashing attributes, in the identification and allocation of attributes, institutions should be guided by the existing definitions. In particular, following the CRR definition of ESG risks, the ESG risk attribute

[3] In May 2022, the European Supervisory Authorities (ESAs) received a request for input from the European Commission requesting each ESA within its sectoral remit and competencies to provide input on the phenomenon of greenwashing, first in the form of progress reports by May 2023, followed by final reports by May 2024, including policy recommendations and a common high-level understanding of greenwashing. For further details, see EBA Final report on greenwashing monitoring and supervision: https://www.eba.europa.eu/sites/default/files/2024-05/a12e5087-8fd2-451f-8005-6d45dc838ffd/Report on greenwashing monitoring and supervision.pdf

should be used for losses that relate specifically to counterparties or invested assets of institutions, i.e. any events related to institution's own practices, in particular related to its own workforce or governance arrangements, would not be captured. Given the scope of operational risk, any credit counterparties or assets where the institution faces risk of default from credit-related transactions, such as loans or bonds, would also be excluded. As a result, the ESG risk attribute may be particularly relevant for Level 1 Event Type 5 *Damage to Physical Assets* (E and S risks) and Event Type 6 *Business Disruption and System Failures* (E, S and G risks), for example:

a. Environmental risks:

    i. *Damage to Physical Assets – Natural Disasters:* Losses that arise from damages to the institution's branches, data centers, or critical infrastructure caused by extreme weather events, such as floods, hurricanes, and wildfires. In this context, all losses related to such weather events should be flagged with ESG risk attribute, without the need to specify whether a specific weather event was due to climate change or not. The effects of climate change on operational risk would be monitored through the frequency and severity of such events and related losses.

    ii. *Business Disruption and System Failures – Infrastructure and System failure:* Losses that arise if the institution relies on its critical infrastructure or processes on third parties that are negatively impacted by physical risk and/or transition risk, which results in operational downtimes for the institution.

b. Social risks:

    i. *Damage to Physical Assets – Other external events:* Losses that arise from damages to the institution's branches, data centers, or critical infrastructure caused by external social factors, like riots, wars.

    ii. In contrast, losses which are caused by internal social factors of the institution (e.g. own inadequate employment practices, inadequate workplace safety) do not fall under the ESG risk attribute.

c. Governance risks:

    i. *Business Disruption and System Failures – Infrastructure and System failure:* Losses that arise from the risk of a third party not providing appropriate services due to having improper governance arrangements, e.g. the third party or its management is involved in illegal practices when performing services for the institution. However, if such practices of the third-party lead to other types of losses than business disruption or system failure, the event may need to be classified into a different category (for instance: *Breaches of statute and regulations* in case the financial institution is fined for not having conducted proper oversight/due diligence).

ii. In contrast, losses which are caused by weaknesses in the institution's own governance arrangements, e.g. employee misconduct, internal fraud, do not fall under this ESG risk attribute.

30. In contrast, greenwashing risk relates directly to the institution's own actions. In this regard, losses from greenwashing risk may be particularly relevant for Event Type 4 (*Clients, Products and Business Practices*) and Event Type 7 (*Execution, Delivery and Process Management*), for example:

i. *Client mistreatment / failure to fulfil duties to customer*: Losses that arise where the institution fails to take sustainability-related product preference of the client into account and mis-sells products that do not meet the desired ESG features.

ii. *Improper distribution marketing, including sale service failure*: Losses due to lawsuits and/or claims from clients due to the inadequate design and marketing of products, such as green financial products when they do not meet the criteria as advertised.

iii. *Breaches of statute and regulations, other than those specifically assigned to other event types or categories*: Losses from supervisory fines or legal claims due to misleading reporting/disclosure of the institution's sustainability efforts, e.g. if the institution claims a much higher reduction in carbon emissions than the actual impact of its financed projects, hence giving misleading signal to stakeholders.

2.2.4 Interaction with Regulation (EU) 2022/2554 (DORA) and rationale for ICT risk attributes

31. These RTS have been aligned with Regulation (EU) 2022/2554 (DORA)[4], which consolidates and upgrades ICT risk requirements as part of the operational risk requirements. In Article 3(14) of DORA, 'cyber-attack' means a malicious ICT-related incident caused by means of an attempt perpetrated by any threat actor to destroy, expose, alter, disable, steal or gain unauthorised access to, or make unauthorised use of, an asset. In Article 2(1) of Regulation (EU) 2019/881 (ENISA Regulation)[5], 'cybersecurity' means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.

[4] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[5] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

32. Among others, DORA requires the recording of all ICT-related incidents and the reporting of major ICT-related incidents (from the financial entities to the competent authorities) on specific time limits and content which are included in the related supplementing technical standards. In particular, the Commission Delegated Regulation (EU) 2025/301 'with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats'[6] requires the financial entities to include the 'type of ICT-related incident' in the intermediate ICT-related incident reporting. The Commission Implementing Regulation (EU) 2025/302 with regard to 'the standard forms, templates, and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat' requires the financial entities to report the 'type of the major ICT-related incident'[7], providing the following choices (multiple):

    i. Cybersecurity related
    ii. Process failure
    iii. System failure
    iv. External event
    v. Payment related
    vi. Other (please specify).

33. When it comes to the loss or the economic impact of the major ICT-related incident, this is required to be reported only in the final report (no later than one month after either the submission of the intermediate report or, where applicable, after the latest updated intermediate report). This should not include financial recoveries or costs that are necessary for the day-to-day operation of the business (e.g. general maintenance costs), and it should consider a list of gross direct and indirect costs and losses which financial entities have incurred as a result of the incident[8].

34. However, it is highlighted that DORA requires financial entities to report only major ICT-related incidents to the competent authorities (i.e. non-major ICT-related incidents may not be reported to the competent authorities). It is further clarified that financial entities are required to record all ICT-related incidents and significant cyber threats (Article 17(2) of DORA).

35. In the draft final RTS, the 'cyber-specific' Level 2 category has been removed because cyber-related losses could cut across different Level 1 event types and Level 2 categories.

[6] Commission Delegated Regulation (EU) 2025/301 of 23 October 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats (OJ L, 2025/301, 20.2.2025, ELI: http://data.europa.eu/eli/reg_del/2025/301/oj).

[7] Commission Implementing Regulation (EU) 2025/302 of 23 October 2024 laying down implementing technical standards for the application of Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to the standard forms, templates, and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat (OJ L, 2025/302, 20.2.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj).

[8] Joint Guidelines on estimation of aggregated annual costs and losses caused by major ICT-related incidents | European Banking Authority

36. In relation to the 'ICT risk' attribute and the need to have a direct and explicit view on the losses stemming from cyber-attacks which form part of the ICT risk, two attributes have been introduced to replace the 'ICT risk' as follows:

    i. 'ICT risk – Other than cyber': As defined in Article 4, paragraph (1), point (52c) of Regulation (EU) 575/2013, excluding losses from cyber-attacks.
    ii. 'ICT risk – Cyber': losses from cyber-attacks as defined in Article 3, point (14) of Regulation (EU) 2022/2554.

37. For both the 'ICT risk' related attributes, institutions should ensure alignment with the major ICT-related incidents reported under DORA. For the attribute 'ICT risk – Cyber' particularly, institutions should ensure consistency with the major ICT-related incidents reported as 'cybersecurity-related' as per the Commission Implementing Regulation (EU) 2025/302.

38. Finally, loss events related to 'ICT third-party service providers' (Article 3(19) of DORA) shall be assigned both the 'ICT risk' and 'Third party risk' attributes. In the same fashion, loss events related to ICT business continuity aspects (Article 11 of DORA) shall be assigned both the 'ICT risk' and 'Business continuity' attributes.

2.2.5 The scheme of the risk taxonomy

39. As consequence of the abovementioned criteria, the scheme of the revised risk taxonomy on operational risk would be as the following:

Level 1 event types	Level 2 categories	Legal risk - Misconduct	Legal risk - Other than misconduct	Model risk	ICT risk - Not related to cyber risk	ICT risk - related to cyber risk	Credit risk (where not included in RWA on credit risk)	Market risk	Third party risk	Environmental, social and governance risk	Greenwashing risk	Business continuity	Retail (including Banking and Retail brokerage)	Trading and sales	Commercial (including Banking and Corporate Finance)	Other business lines
Internal Fraud	Bribery and Corruption	Yes														
Internal Fraud	Internal fraud committed against the institution	Yes														
Internal Fraud	Internal fraud com-mitted against other stakeholders	Yes														
External Fraud	Fraud committed by institution's clients															
External Fraud	Fraud not committed by institution's clients															
External Fraud	Data theft and manipulation															
External Fraud	Robbery, Burglary and theft of physical assets															
Employment Practices and Workplace Safety	Inadequate Employment practice															
Employment Practices and Workplace Safety	Inadequate workplace safety															
Clients, Products and Business Practices	Client mistreatment / failure to fulfil duties to customer	Yes														
Clients, Products and Business Practices	Data privacy breach / confidentiality mismanagement	Yes														
Clients, Products and Business Practices	Improper market practices, anti-trust / anti-competition	Yes														
Clients, Products and Business Practices	Improper distribution marketing, including sale service failure	Yes														
Clients, Products and Business Practices	Financial Crime	Yes														
Clients, Products and Business Practices	Breaches of statute and regulations, other than those specifically as-signed to other event types or categor	Yes														
Clients, Products and Business Practices	Improper product and service design	Yes														
Clients, Products and Business Practices	Model methodology	Yes		Yes												
Damage to Physical Assets	Natural disasters															
Damage to Physical Assets	Other external events															
Business Disruption and System Failures	Infrastructure and System failure															
Business Disruption and System Failures	Business disruption															
Execution, Delivery and Process Management	Processing / execution failures															
Execution, Delivery and Process Management	Client account mismanagement															
Execution, Delivery and Process Management	Rights / obligation failures															
Execution, Delivery and Process Management	Data management															
Execution, Delivery and Process Management	Model implementation and use			Yes												

'Yes' means that the total loss of that Level 1 or 2 category should automatically receive the attribute.

'Gray' means that no loss of that Level 1 or 2 category can receive the attribute.

'White' means that losses of that Level 1 or 2 category may receive the attribute, and institutions will report the exact amount of attributed losses.

2.2.6 Rationale for the exclusion of causes

40. One of the additional dimensions considered for reviewing the Level 2 categorisation is the 'cause' of the losses. However, the cause of the losses was not included in these draft RTS because the proposed revision of Level 1 event types and Level 2 categories, as well as the introduction of flags, already provides a significant level of details on each operational risk event which would also allow institutions and competent authorities to identify the main causes triggering the event itself.

2.2.7 Methodology for the classification of loss events included in the loss data set

41. In line with Article 317(9) of the CRR, the EBA is also mandated to develop a methodology to classify the loss events in the loss data set. There are several concepts typical for operational risk loss events, that are not defined in the CRR, such as rapidly recovered loss events, events falling in multiple categories or event types, and loss events due to legal proceedings. These are clarified in the draft RTS in order to get a fully harmonised classification scheme and avoid that the misinterpretation of loss events affects the amount of the annual operational risk loss to be reported by institutions.

2.3 Draft regulatory technical standard for the specification of the conditions under which the calculation of the annual operational risk loss may be deemed 'unduly burdensome'

42. The first paragraph of Article 316(1) of the CRR requests institutions with a BI equal to or higher than EUR 750 million to calculate their annual operational risk loss. The second subparagraph of Article 316(1) of the CRR allows for a derogation from the first subparagraph: competent authorities may grant to institutions with a BI between EUR 750 million and EUR 1 billion a waiver from the calculation of the annual operational risk loss, provided that the institution has demonstrated that it would be 'unduly burdensome' for it to apply the first subparagraph.

43. Article 317(2) of the CRR states that the institution's loss data set needs to capture all operational risk events stemming from all the entities that are part of the scope of consolidation pursuant to Part One, Title II, Chapter 2 of the CRR. From the combined reading of Articles 316(1), first and second subparagraphs, and Article 317(2), the derogation envisaged in Article 316(1) second subparagraph applies to the whole institution, as opposed to only some parts (entities or activities) within it. If the institution has not received the waiver pursuant to Article 316(1) second subparagraph, the loss data set needs to encompass all the parts of the institution.

44. The CRR 3 uses the term 'institution' when it refers to either an institution on a solo basis, or a banking group. For the draft RTS, the term 'institution' has the same meaning as in the CRR 3.

2.3.1 Level of application of the waiver

45. Article 317(2) of the CRR states that the institution's loss data set needs to capture all operational risk events stemming from all the entities that are part of the scope of consolidation pursuant to Part One, Title II, Chapter 2 of the CRR. From the combined reading of Article 316(1), first and second subparagraphs, and Article 317(2), the derogation envisaged in Article 316(1) second subparagraph applies to the whole institution, as opposed to only some parts (entities or activities) within it. If the institution has not received the waiver pursuant to Article 316(1) second subparagraph, the loss data set needs to encompass all the parts of the institution.

46. The CRR 3 uses the term 'institution' when it refers to either an institution on a solo basis, or a banking group. For the draft RTS, the term 'institution' has the same meaning as in the CRR 3.

2.3.2 Situations where calculating the annual operational risk loss could be considered 'unduly burdensome'

47. There might be cases where an institution is not able to promptly calculate the annual operational risk loss for some of the institution's entities or activities. This might be due to mergers and acquisitions (M&As), a temporary breach of the EUR 750 million threshold, or the set-up of a bridge institution according to Article 40 of Directive 2014/59/EU1 (BRRD).

48. Firstly, in the context of M&As, institutions may breach the EUR 750 million threshold for the BI due to this type of operations, but do not exceed EUR 1 billion. In addition, institutions may face hurdles in incorporating loss data of the merged or acquired entities, or activities into the loss data set. In this case, the calculation of the annual operational risk loss may be unduly burdensome, and the institution may receive a waiver regarding this calculation for a maximum of three years. After three years, or earlier if the institution can promptly implement the inclusion of the loss data concerning merged or acquired entities, or activities in the loss data set, the waiver to calculate the annual operational risk loss should be withdrawn. In addition, if at least one institution involved in the merger or acquisition was calculating the operational risk loss before the merger or the acquisition, the institution may receive a waiver concerning the calculation of the operational risk loss for two years. If all the institutions involved in the merger or acquisition were calculating the operational risk loss before the operation, the waiver should not be granted.

49. Secondly, institutions may also temporarily breach the EUR 750 million threshold for the BI, but do not exceed EUR 1 billion, for instance due to unexpected losses or profits, or a temporary increase in activity. In this case, it may be deemed as unduly burdensome to require the calculation of the operational risk loss when the institution breaches the abovementioned threshold for no more than four consecutive reporting dates, or eight non-consecutive reporting dates in the previous twenty consecutive reporting dates.

50. Finally, Article 40 of the BRRD allows for the creation of a bridge institution in case of resolution of an institution. For the bridge institution, it may be disproportionate to calculate the operational risk loss since it will have to deal with assets and liabilities of the institution under resolution.

2.4 Draft regulatory technical standards for the specification on how institutions shall determine the adjustments to their loss data set following the inclusion of losses from merged or acquired entities or activities under Article 321(2) of the CRR

51. Article 321(1) of the CRR states that institutions shall include in the loss data set losses observed during a ten-year period prior to an acquisition or merger stemming from merged or acquired entities or activities as soon as the business indicator items related to those entities or activities are included in the institution's business indicator calculation. Article 321(2) mandates the EBA to develop a draft RTS to specify how institutions shall determine the adjustments to their loss data set following the inclusion of the losses from merged or acquired entities or activities.

52. The provisions of Article 321(1) of the CRR apply to all institutions that have to calculate the annual operational risk loss according to Article 316(1), first subparagraph of the CRR.

2.4.1 Clarifications on how to carry out adjustments to the loss data set in the context of M&A of entities and/or activities

53. When the currency of the acquired/merged entity or activity is different, Institutions may perform mergers and acquisitions, or include activities, for entities or activities in a currency which is different from the one of the reporting institutions. In this case, the loss data set of the merged or acquired entities or activities should be included in the institution's loss data set by converting the values into the currency of the reporting institution applying, for each year of the ten-year window, the exchange rate used at the relevant year of the financial statement. Following operations of mergers or acquisitions or inclusion of activities, institutions may not be able to readily incorporate losses stemming from these operations in the loss data set. In order to avoid an underestimation of the institution's losses, institutions should calculate the annual loss coverage of reported losses of the entire institution using the BI as the proxy, by calculating the ratio of covered losses to the total losses.

54. Since the use of the proxy provides an estimation of the institution's losses, its use should be intended as temporary, and the institution is expected to adjust the loss data set following the inclusion of losses from merged or acquired entities or activities within one year from the completion of the operation.

55. In some cases, the acquiring institution may not be able to allocate the annual operational risk loss for part or all the acquired or merged institution or activities according to the risk taxonomy developed according to Article 317(9) of the CRR. This situation may arise due to the lack of

data of sufficient quality, or incomplete loss data set. In this case, the institution should allocate losses according to the distribution of losses in the reporting institution. The institution is expected to allocate the annual operational risk loss for part or all the acquired or merged institution or activities within one year from the completion of the merger or acquisition, or of the inclusion of the activities.

3. Draft regulatory technical standards for 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 under Article 317(9) of the CRR, for the specification of the conditions under which the calculation of the annual operational risk loss may be deemed 'unduly burdensome' under Article 316(3) of the CRR and for the specification on how institutions shall determine the adjustments to their loss data set following the inclusion of losses from merged or acquired entities or activities under Article 321(2) of the CRR

COMMISSION DELEGATED REGULATION (EU) …/…

of XXX

supplementing Regulation (EU) 2013/575 of the European Parliament and of the Council with regard to regulatory technical standards for establishing a risk taxonomy on operational risk and a methodology to classify the loss events included in the loss data set under Article 317(9) of that Regulation, for the specification of the conditions under which the calculation of the annual operational risk loss may be deemed 'unduly burdensome' under Article 316(3) of that Regulation and for the specification on how institutions shall determine the adjustments to their loss data set following the inclusion of losses from merged or acquired entities or activities under Article 321(2) of that Regulation

(Text with EEA relevance)

THE EUROPEAN COMMISSION,
Having regard to the Treaty on the Functioning of the European Union,
Having regard to Regulation (EU) No 575/2013 as amended by Regulation (EU) 2024/1623 of the European Parliament and of the Council of 31 May 2024 as regards requirements for credit risk, credit valuation adjustment risk, operational risk, market risk and the output floor[9], and in particular Article 316(3), Article 317(9) and Article 321(2), third subparagraph thereof,
Whereas:

(1) International standards on operational risk require loss events to be classified into seven event types. To comply with those standards, the operational risk taxonomy referred to in Article 317(9) of Regulation (EU) 575/2013 should be based on the same event types.

(2) To obtain a sufficiently granular classification system, the operational risk taxonomy should also include a second level of classification, based on the industry best practices. Accordingly, the operational risk taxonomy should organise loss data events in Level 1 event types, representing the macro-events to which a loss event should be assigned, and Level 2 categories, listing in more detail the features of the corresponding Level 1 event types. The design and description of Level 2 categories is developed according to international standards and industry best practices, and aim to foster harmonisation in the recording of loss events.

(3) In order to provide the complete picture of the losses of an institution, the construction of the operational risk taxonomy in Level 1 event types and Level 2 categories should be designed to make them mutually exclusive and collectively exhaustive, without envisaging any residual category.

(4) Though Level 1 event types and Level 2 categories are exhaustive with reference to operational risk losses, some loss events may be attributable to a supplementary description in addition to its assignment to the relevant Level 1 event type and

[9] OJ L, 2024/1623, 19.6.2024.

Level 2 category. In order to enrich the recording of information available on loss events, institutions should be required to assign one or more attributes to these events, when appropriate. Given their nature, attributes should not be designed to make them mutually exclusive and collectively exhaustive, thus multiple attributes may be assigned to a single loss event, such as loss events related to 'ICT third-party service providers' as defined in Article 3, paragraph 19 of Regulation (EU) 2022/2554, which should be assigned both the 'ICT risk' and 'Third party risk' attributes.

(5) In order to adequately describe the losses incurred by an institution, only losses that are relevant for the calculation of the annual operational risk loss should be recorded in the loss data set, while institutions should not include in the loss data set losses that are recovered within five working days.

(6) In order to allow for an effective supervision of the operational risk, institutions should be required to assign loss events to Level 1 event types from the ten years preceding the date of entry into force of this Regulation and, on a voluntary basis, to assign loss events to Level 2 categories and attributes from one year preceding the date of entry into force of this Regulation.

(7) The challenges to the calculation of the annual operational risk loss are mostly due to the short timing available for the implementation of the appropriate systems and procedures, and the effort to put in place is not unduly burdensome when the institution is given an appropriate time span.

(8) Mergers and acquisitions may lead an institution to the obligation to calculate the annual operational risk loss due to the increased size of the business indicator. Furthermore, the challenges stemming from the integration of the merged or acquired entities may result in an effort needed to calculate the operational risk losses which is unduly burdensome, thus an appropriate time span should be given to institutions before complying with the requirement to calculate the annual operational risk loss.

(9) Institutions may temporarily report a business indicator equal to or higher than EUR 750 million due to transitory circumstances, and it would be unduly burdensome for these institutions to calculate the annual operational risk loss when exceeding the threshold is only a temporary exception within a certain time frame.

(10) In specific circumstances, bridge institutions may be set up to manage the resolution of institutions. Given the specificity of the bridge institutions and their temporary nature, it would be unduly burdensome for these institutions to calculate the annual operational risk loss.

(11) Acquired or merged entities or activities may record losses using a risk taxonomy which is different from the one of the reporting institution. In order to ensure the comparability and consistency of the data, the reporting institution should reclassify the losses of the acquired or merged entities using the risk taxonomy referred to in Article 317 of Regulation (EU) 575/2013.

(12) The losses of the acquired or merged entities or activities may be in a currency which is different from the one of the reporting institution, therefore these losses should be incorporated in the losses of the reporting institution using, for each of the ten-years window, the exchange rate used at the end of the relevant year.

(13) Merged or acquired entities or activities may not record losses, or may record losses using a risk taxonomy that is different from that referred to in Article 317, paragraph 9 of Regulation (EU) 575/2013, because they are not mandated by the applicable law to build a loss data set according to Article 317 of that Regulation. It is also possible that merged or acquired entities or activities were not in scope of Article 317 of that Regulation for each of the 10 years prior to the acquisition or the merger. When this situation arises, institutions should calculate the annual operational risk loss using the reported losses for which data is available, adjusting the result for the coverage rate or the reported losses compared to the whole institution.

(14) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Banking Authority.

(15) The European Banking Authority conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the Banking Stakeholder Group established under Article 37 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council[10],

HAS ADOPTED THIS REGULATION:

CHAPTER 1

Risk taxonomy on operational risk

Article 1
Classification of loss events

1. Institutions shall classify each loss event into a single Level 1 event type in accordance with Article 2 and into a single Level 2 category in accordance with Articles 3 to 9. In case a loss event falls under multiple Level 1 event types or multiple Level 2 categories, it shall be classified into the most relevant Level 1 event type or Level 2 category.
2. Institutions shall assign to each loss event all the applicable attributes in accordance with Article 10.
3. Institutions shall not include in the loss data set losses that are fully recovered within five working days. Where the recovery is partial, institutions shall include in the gross loss referred to in Article 318, paragraph (1) of Regulation (EU) 575/2013 only the part of the loss that is not recovered within five working days.
4. Loss events due to legal proceedings shall be considered losses due to all legal disputes and settlements, including both mandated court settlements and out of court disputes and settlements.

[10] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

Article 2
Level 1 classification

Institutions shall classify each loss event in one of the following Level 1 event types:

Level 1 event type classification	Description	Reference number
Internal Fraud	Losses due to acts of a type intended to defraud and misappropriate property, excluding diversity/discrimination events, which involves at least one internal party (i.e. a party with a direct relationship to the institution or for which the institution is jointly liable), including instances where the internal party is acting in collusion with external parties.	1
External Fraud	Losses due to acts of a type intended to defraud and misappropriate property, committed by an external party without the involvement of an internal party.	2
Employment Practices and Workplace Safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/discrimination events towards employees.	3
Clients, Products and Business Practices	Losses other than fraud arising from failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), from business practices or from the nature or design of a product.	4
Damage to Physical Assets	Losses arising from loss or damage to physical assets, employees or affiliates of the institution, public assets or non-affiliated people for which the institution is liable,	5

	due to natural disasters or other events, including accidents, wilful damage, war, civil disturbance, riots and terrorism.	
Business Disruption and System Failures	Losses arising from disruption of business or system failures.	6
Execution, Delivery and Process Management	Losses from failed transaction processing or process management and data management, from relations with trade counterparties, vendors and regulatory and tax authorities.	7

Article 3

Level 2 classification for Level 1 event type Internal Fraud

Institutions shall classify each loss event classified as Internal Fraud in accordance with Article 2 into one of the following Level 2 categories:

Internal Fraud Level 2 classification	Description	Reference number
Bribery and Corruption	Bribery or corruption from an internal party of the institution.	1.1
Internal Fraud Committed Against the Institution	Fraud committed by an internal party against the institution. It encompasses theft or manipulation of data and rogue trading events, including those perpetrated through insider trading and manipulation of positions, risks and profit and loss accounts.	1.2
Internal Fraud Committed Against Other Stakeholders	Fraud committed by an internal party against the institution's external parties, including clients and third parties. It encompasses theft or manipulation of data and rogue trading events, including those perpetrated through insider trading and manipulation of positions, risks and profit and loss accounts.	1.3

Article 4
Level 2 classification for Level 1 event type External Fraud

Institutions shall classify each loss event classified as External Fraud in accordance with Article 2 into one of the following Level 2 categories:

External Fraud Level 2 classification	Description	Reference number
Fraud Committed by Institution's Clients	Fraudulent acts not relating data theft or data manipulation that have been committed by a client of the institution, even in collusion with another person.	2.1
Fraud not Committed by Institution's Clients	Fraudulent acts not relating data theft or data manipulation that have not been committed by a client of the institution, such as by means of the identity of another ignorant person.	2.2
Data Theft and Manipulation	Data being stolen or maliciously manipulated by any means, such as cyber-attacks. This covers all types of data, e.g. client data, employee data, and the institution's proprietary data.	2.3
Robbery, Burglary and Theft of Physical Assets	Robbery, Burglary and theft of physical assets by an external party	2.4

Article 5
Level 2 classification for Level 1 event type Employment Practices and Workplace Safety

Institutions shall classify each loss event classified as Employment Practices and Workplace Safety in accordance with Article 2 into one of the following Level 2 categories:

Employment Practices and Workplace Safety Level 2 classification	Description	Reference number
Inadequate Employment Practice	Losses arising from breach of employment legislation or regulatory requirements (e.g. actual or perceived mistreatment of employees which can be	3.1

	traced to a regulatory breach, like unfair dismissal, harassment); ineffective employment relations (including industrial action, like strikes, tribunals, and ineffective union/employee group relations management); diversity and discrimination towards employees.	
Inadequate Workplace Safety	Losses arising from ineffective workplace safety and breach of employees' health and safety rules.	3.2

Article 6

Level 2 classification for Level 1 event type Clients, Products and Business Practices

Institutions shall classify each loss event classified as Clients, Products and Business Practices in accordance with Article 2 into one of the following Level 2 categories:

Clients, Products and Business Practices Level 2 classification	Description	Reference number
Client Mistreatment / Failure to Fulfil Duties to Customer	Inappropriate behaviour towards customer and failure to respect and comply with duties to customers, either actual or potential.	4.1
Data Privacy Breach / Confidentiality Mismanagement	Improper disclosure or misuse of confidential information.	4.2
Improper Market Practices, Anti-Trust / Anti-Competition	Conducting business activities in breach of trading rules and standards, including all types of market abuse and manipulation. Violations of antitrust or competition laws where the institution fails to act in accordance with clients' best interest	4.3
Improper Distribution Marketing, including Sale Service Failure	Improper/inadequate means of distribution of products and services and improper/inaccurate direct marketing practices.	4.4

	Sale service failure includes both pre-sales service failure and post-sales service failure. Pre-sales failure is inadequate/improper services to clients ahead of sales, including mis-selling and failure to provide adequate advice. Post-sales failure refers to inadequate/improper services to clients after sales, including the failure to respond to client complaints regarding poor sales services within the timelines defined by the regulator	
Financial Crime	The risk of money laundering, KYC failure and sanctions violations. It encompasses: - failure to comply with the restrictions imposed by sanctions, including operational risk events due to mistaken transactions involving sanctioned countries - engagement in money laundering and terrorism financing, including failures in KYC process.	4.5
Breaches of Statute and Regulations, other than Those Specifically Assigned to Other Event Types or Categories	Breach of any legal or regulatory obligations, including the institution's legal obligations and the obligations from regulatory and tax authorities. It encompasses - operating without the necessary licence, certification or registration - tax evasion Where tax evasion is committed to consciously circumvent the tax regulation, the loss event shall be assigned to event 1.3	4.6
Improper Product and Service Design	Flaws in design of products or services targeted at clients such that the design of a product/service does not meet client's needs.	4.7
Model Methodology	Losses due to errors in the model itself, including the model design, incorrect formulae, methodology and underlying assumptions. If Artificial Intelligence (AI) systems are components of the model, then an error due to this technology could fall under the scope of model risk.	4.8

Article 7

Level 2 classification for Level 1 event type Damage to Physical Assets

Damage to Physical Assets Level 2 classification	Description	Reference number
Natural Disasters	Losses due to natural disasters, including pandemic events.	5.1
Other External Events	Losses due to other events, including accidents, wilful damage, war, civil disturbance, riots and terrorism. Business disruption events, such as those stemming from workforce availability, should not be mapped in this category.	5.2

Article 8

Level 2 classification for Level 1 event type Business Disruption and System Failures

Institutions shall classify each loss event classified as Business Disruption and System Failures in accordance with Article 2 into one of the following Level 2 categories:

Business Disruption and System Failures Level 2 classification	Description	Reference number
Infrastructure and System Failure	Infrastructure and System failure due to Internal application failures, internal and network and information systems and support failures, utility and external support failures, infrastructure failures, ICT change programmes failures.	6.1
Business Disruption	Business Disruption due to workforce availability, workplace availability.	6.2

Article 9

Level 2 classification for Level 1 event type Execution, Delivery & Process Management

Institutions shall classify each loss event classified as Execution, Delivery and Process Management in accordance with Article 2 into one of the following Level 2 categories:

Execution, Delivery and Process Management Level 2 classification	Description	Reference number
Processing/Execution Failures	Failure to process, manage and execute transactions (such as fat finger losses) and/or other processes (such as change programmes, different from the ICT ones) correctly and/or appropriately.	7.1
Client Account Mismanagement	Inadequate management of client portfolio/investments, including unapproved access given to accounts, incorrect client records (loss incurred), negligent loss or damage to client assets.	7.2
Rights/Obligation Failures	Failure to follow the appropriate procedure for handling legal processes. Failure to manage contractual and non-contractual rights/obligations correctly. It includes all execution errors pertaining to legal procedures and processes, including in reporting to external parties, such as tax and regulatory authorities. It does not include breaches of the organisation's legal obligations, legal disputes and litigations.	7.3
Data Management	Failing to appropriately manage and maintain data, including all types of data, for example, client data, employee data, and the organisation's proprietary data. This excludes breaches of data privacy and confidentiality mismanagement.	7.4
Model Implementation and Use	Incorrectly implementing a model, even though the model may be correct.	7.5

	Using a model in an incorrect context, even though the model may be correct and correctly implemented.	

Article 10
Attributes

1. Institutions shall assign to each loss event all the applicable of the following attributes:

Attributes	Description
Legal risk – Misconduct	As defined in Article 4, paragraph 52a, point (d) of Regulation (EU) 575/2013.
Legal risk – Other than Misconduct	As defined in Article 4, paragraph 52a, points (a) to (c) and (e) to (g) of Regulation (EU) 575/2013.
Model Risk	As defined in Article 4, paragraph 52b of Regulation (EU) 575/2013.
ICT Risk – not Related to Cyber	As defined in Article 4, paragraph 52c of Regulation (EU) 575/2013, excluding losses from cyber-attacks.
ICT Risk – Related to Cyber	Losses induced by cyber-attacks as defined in Article 3, point (14) of Regulation (EU) 2022/2554.
Credit Risk (Where not included in RWA on Credit Risk)	Operational risk losses related to credit assets such as credit frauds (committed by the client on its own account or by a third-party through identity theft), unenforceable credit contracts or collateral failures, that have been unpaid and are not accounted for in the risk-weighted exposure amount for credit risk.
Market Risk	At least the following events, and the related losses, are classified as operational risk related to financial transactions and market risk: a. events due to operational and data entry errors, including the following:

	i. failures and errors during the introduction or execution of orders; ii. loss of data or misunderstanding of the data flow from the front to the middle and back offices of the institution; iii. errors in classification; iv. incorrect specification of deals in the term-sheet, including errors related to the transaction amount, maturities and financial features; b. events due to failures in internal controls, including the following: i. failures in properly executing an order to unwind a market position in case of adverse price movements; ii. unauthorised positions taken in excess of allocated limits, irrespective of the type of risk they relate to; c. events due to inadequate data quality and unavailability of IT environment, including technical unavailability of access to the market resulting in an inability to close contracts.
Third-Party Risk	Losses that may arise for an institution in relation to its use of services provided by third-party service providers or by subcontractors of the latter, including through outsourcing arrangements. These losses encompass those due to failures in managing third party relationships and risks appropriately, such as developing and maintaining an adequate third-party control framework (e.g. due diligence including selection of third-party service providers, ongoing monitoring) or defining and implementing adequate contractual arrangements/SLAs.
Environmental, Social and Governance Risks	Losses that may arise from environmental risks, as defined in Article 4, paragraph 52e-g of Regulation (EU) 575/2013. Losses that may arise from social and governance risks, as defined in Article 4, paragraph 52h-i of Regulation (EU) 575/2013.
Greenwashing Risk	The scope of application includes Greenwashing risk, with reference to the losses arising from practices whereby sustainability related statements, declarations, actions, or communications do not clearly and fairly reflect the underlying

	sustainability profile of an entity, a financial product, or financial services. These practices may be misleading to consumers, investors or other market participants.
Business Continuity	Failure to provide and maintain appropriate business continuity management and event management framework (also encompassing ICT business continuity and ICT recovery and response aspects as per the Regulation (EU) 2022/2554) including inadequate business continuity plans.
Retail (including Banking and Retail Brokerage)	Operational events and losses linked to retail clients, including: a. natural persons; b. SMEs (small and medium-sized enterprises) as defined in Article 5, paragraph 9, of Regulation (EU) 575/2013. The list of activities for this attribute includes: a. retail and private banking: lending and deposits, transactional and saving accounts, ATMs services, banking services, financial leasing, guarantees and commitments, trusts and estates, investment advice, card services (debit and credit cards, merchant/commercial/corporate cards, private labels); b. retail brokerage: reception, transmission and execution of client orders, placing of financial instruments without a firm commitment basis.
Trading and Sales	Operational events and losses linked to activities such as flow business and sales, brokerage, market making, treasury, position taking, and proprietary positions managed by trading desks, as defined in Article 4, paragraph 144 of Regulation (EU) 575/2013. The list of products for this attribute includes: a. equities: equity portfolios and indices; b. fixed income and credit trading; c. foreign exchange; d. commodities and energy products; e. money market, funding, repos and securities lending; f. derivatives.

Commercial Banking	Operational events and losses linked to activities such as lending and deposits, guarantees, leasing and factoring, trade finance, project finance, real estate.
Other Business Lines (including Corporate Finance, Payment and Settlement, Asset Management, Agency Services, Corporate Items)	This attribute collects the remaining operational events and losses linked to activities, other than those mentioned in the Retail, Trading and Sales, and Commercial Banking attributes, such as the following: a. corporate finance: mergers and acquisitions, underwriting, privatisations, securitisation, IPO and private placements, advisory services, municipal and government finance, merchant banking; b. payments and settlements for external clients: payments and collections, funds transfer, cash and securities clearing and settlement. Payment and settlement losses related to a bank´s own activities would be incorporated in the affected business line; c. agency services for the account of clients: custody services (escrow, depository receipts, corporate actions, etc.), corporate trust and agency (issuer and paying agents); d. asset management: discretionary and non-discretionary fund management, including portfolio management (pooled, segregated, retail, institutional, closed, open, private equity); e. corporate items: for purely corporate level items, such as those affecting the Board of Directors, misreporting financial statements, or other events that can only be categorised at corporate centre.

2. By way of derogation from paragraph 1, institutions shall assign to each loss event at least one attribute among ‘Retail (including banking and retail brokerage)’, ‘Trading and sales’, ‘Commercial banking’ and ‘Other business lines (including corporate finance, payment and settlement, asset management, agency services, corporate items)’.

3. By way of derogation from paragraph 1, the attributes ‘Legal risk – Misconduct’, ‘Legal risk – Other than misconduct’ and ‘Model risk’ shall be mapped to Level 1 event types and Level 2 categories in accordance with the Annex to this regulation.

Article 11
First application

1. At first application, institutions shall assign loss events to the relevant Level 1 event types in accordance with Article 2 from the ten years preceding the date of entry into force of this Regulation.

2. Institutions may assign loss events to the relevant Level 2 categories in accordance with Article 2 from at least one year preceding the date of entry into force of this Regulation.

3. Institutions may assign attributes to loss events in accordance with Article 10 from at least one year preceding the date of entry into force of this Regulation.

CHAPTER 2

Conditions under which the calculation of the annual operational risk loss may be deemed 'unduly burdensome'

Article 12
Mergers and acquisitions

1. Where, due to a merger or acquisition, the business indicator of an institution equals or exceeds EUR 750 million, but does not exceed EUR 1 billion, the calculation of the operational risk loss shall be deemed as unduly burdensome for the purposes of Article 316, paragraph 1, second subparagraph of Regulation (EU) 575/2013 for up to three years following the legal finalisation of the merger or acquisition.
2. The period referred to in paragraph 1 shall be reduced to up to two years following the legal finalisation of the merger or acquisition if at least one, but not all, of the institutions involved in the merger or acquisition calculated the operational risk loss the year prior to the operation.
3. If all of the institutions involved in the merger or acquisition calculated the operational risk loss the year prior to the operation, the calculation of the operational risk loss of the institution resulting from the merger or acquisition shall not be deemed as unduly burdensome.

Article 13
Business indicator temporarily equal to or exceeding EUR 750 million and not exceeding EUR 1 billion

The calculation of the operational risk loss shall be deemed as unduly burdensome for the purposes of Article 316, paragraph 1, second subparagraph of Regulation (EU) 575/2013, for institutions whose business indicator is equal to or exceeding EUR 750 million, but not exceeding EUR 1 billion, for no more than four consecutive reporting dates, or for no more than eight reporting dates in the preceding twenty reporting dates.

Article 14
Bridge institution referred to in Article 40 of Directive 2014/59/EU

The calculation of the operational risk loss shall be deemed as unduly burdensome for the purposes of Article 316, paragraph 1, second subparagraph of Regulation (EU) 575/2013, for bridge institutions referred to in Article 40 of Directive 2014/59/EU.

CHAPTER 3

Adjustments to the loss data set following the inclusion of losses from merged or acquired entities or activities

Article 15
Adjustments to the loss data set related to calculation of losses and risk taxonomy

Losses stemming from merged or acquired entities or activities shall be recorded in the loss data set of the reporting institution with the necessary adjustments to ensure compliance with the requirements laid down in Articles 317 and 318 of Regulation (EU) 575/2013.

Article 16
Adjustments to the loss data set due to currency differences

Where the currency of the merged or acquired entities or activities is different from the currency of the acquiring institution, losses stemming from merged or acquired entities or activities shall be included in the loss data set applying, for each of the ten-year window, the exchange rate used at the end of the relevant year in the institution's financial statement.

Article 17
Calculation of the losses when the acquiring or merging institution is not able to promptly integrate the loss data set of the acquired or merged institution or activities

1. When the merged or acquired entities or activities have not established or maintained a loss data set because they are not in scope of Article 317 of Regulation (EU) 575/2013, the acquiring institution can use the following formula to calculate the annual operational risk loss referred to in Article 316 of that Regulation.

$$Annual\ operational\ risk\ loss = \frac{Reported\ Losses}{Coverage\ of\ Reported\ Losses}$$

where:

reported losses = the annual operational risk loss of the entities or activities able to report the annual operational risk loss

coverage of reported losses = $\frac{Business\ Indicator\ of\ entities\ or\ activities\ able\ to\ report\ the\ annual\ operational\ risk\ losses}{Business\ Indicator\ of\ the\ institution}$

business indicator of the institution = the business indicator resulting from the consolidation of the acquiring institution including the acquired or merged entities, or activities.

2. The acquiring entity can use the formula provided in paragraph 1 to calculate the annual operational risk loss for up to 10 years prior to legal finalisation of the acquisition or merger.

3. By way of derogation from paragraph 1, when the merged or acquired entities or activities are in scope of Article 317 of Regulation (EU) 575/2013, but the acquiring institution is not able to promptly adjust their loss data set, it can use the formula provided in that paragraph to calculate the annual operational risk loss referred to in Article 316 of that Regulation for up to two years following the legal finalisation of the acquisition or merger.

4. When the acquiring institution is not able to promptly allocate the annual operational risk loss for part or all of the acquired or merged institution or activities according to the mapping of historical loss data referred to in Article 317, paragraph 7 of Regulation (EU) 575/2013, it shall allocate, for a maximum of two years following the legal finalisation of the acquisition or merger, losses according to the distribution of losses in the reporting institution.

Article 18
Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission
The President
§§§

ANNEX

Attributes	Mapping to Level 1 event types and Level 2 categories
Legal Risk – Misconduct	1. Loss events classified into the following Level 1 event types and Level 2 categories shall always be assigned the attribute 'Legal Risk – Misconduct': 1.1, 1.2, 1.3, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8 2. Loss events classified into Level 1 event types and Level 2 categories different than those in point (1) shall not be assigned the attribute 'Legal risk - Misconduct'.
Legal Risk – Other than Misconduct	3. Loss events classified into the following Level 1 event types and Level 2 categories may be assigned the attribute 'Legal Risk – Other than Misconduct': 2.1, 2.2, 2.3, 2.4, 3.1, 3.2, 5.1, 5.2, 6.1, 6.2, 7.1, 7.2, 7.3, 7.4, 7.5 4. Loss events classified into Level 1 event types and Level 2 categories different than those in point (3) shall not be assigned the attribute 'Legal Risk – Other than Misconduct'.
Model Risk	5. Loss events classified into the following Level 1 event types and Level 2 categories shall always be assigned the attribute 'Model Risk': 4.8, 7.5 6. Loss events classified into the following Level 1 event type and Level 2 category may be assigned the attribute 'Model Risk': 7.4

	7. Loss events classified into Level 1 event types and Level 2 categories different than those in points (6) and (7) shall not be assigned the attribute 'Model Risk'.

4. Accompanying documents

4.1 Draft cost-benefit analysis / impact assessment

The current session on impact assessments tries to assess the impact of implementing the EBA proposals that address the following mandates of the CRR 3/CRD 6:

- on 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 under Article 317(9) of Regulation (EU) 575/2013;

- on specifying how institutions shall determine the adjustments to their loss data set following the inclusion of losses from merged or acquired entities or activities under Article 321(2) of Regulation (EU) 575/2013;

- on specifying the condition of 'unduly burdensome' for the calculation of the annual operational risk loss under Article 316(3) of Regulation (EU) 575/2013.

While the last of the above-listed EBA deliverables can be assessed based on already submitted data, the first two can only be assessed on a high-level qualitative basis, based on expert views that comply with the strategic objectives of the EBA.

4.2 Draft cost-benefit analysis/impact assessment on 'Establishing a risk taxonomy' (Article 317(9) of the CRR) and on the 'Adjustments to loss dataset due to mergers and acquisitions' (Article 321(2) of the CRR)

A. Policy objectives

The strategic objective of the EBA technical standards, for the first deliverable above, is to provide sufficient provisions for building a methodology for the classification of losses in a consistent way, while the operational objective, i.e. the means for achieving the strategic objective, is to provide a taxonomy for the classification of losses.

The specific objective of the EBA technical standards, for the second deliverable above, is to provide sufficient provisions for providing clarifications to the institutions on how institutions shall determine the adjustments to their loss data due to mergers, acquisitions, and to activities under Article 321(2) of Regulation (EU) 575/2013.

In doing so, the EBA is confronted with some operational challenges:

(a) It must request the necessary information by using, as much as possible, the existing information for the taxonomy to avoid burdening credit institutions;
(b) It must harmonise, across the EU, the best practices; and,
(c) The proposals should not have a detrimental effect on the total economic cost resulting from the cost of regulatory capital and the operational cost of the preferred solutions.

B. Cost-benefit analysis for (a) operational risk taxonomy for the classification of loss events and (b) adjustments to loss databases due to mergers and acquisitions

Due to the nature of the mandate, there was no leeway for developing the different options as to draft the RTS in question. Instead, the deliverables focused on providing the most detailed specifications as possible to facilitate institutions to follow a harmonised approach for the classification of losses and the application of the necessary adjustments of the loss database in cases of mergers and acquisitions.

To this end, the current impact assessment is limited to be conducted on qualitative grounds and based on expert views and past experiences. To this end, the cost is negligible, for both deliverables in question, and is limited to the implementation of the suggested proposals from the affected institutions. More specifically, the cost is limited to the implementation of the methodology for the second-level taxonomy of losses and for the retroactive aggregation/integration of loss databases for the past years.

4.3 Draft cost-benefit analysis/impact assessment on 'Condition of unduly burdensome' (Article 316(3) of the CRR)

The current section intends to provide an impact assessment to quantitatively justify the conditions of defining the 'unduly burdensome' for the purposes of Article 316(1) of that Regulation. The analysis presented herein is based on data collected via the QIS templates that serve the purposes of the EBA mandatory exercise for the Basel III monitoring exercise. The data refer to the period December 2015 to December 2022 and include a sample of 228 banks that participated in the Basel III monitoring exercise for at least one reference date over the specified period.

A. Problem identification

Article 316(1) of the CRR 3 requires institutions with a business indicator equal to or exceeding EUR 750 million shall calculate their annual operational risk loss as the sum of all net losses over a given financial year, calculated in accordance with Article 318(1), that are equal to or exceed the loss data thresholds (EUR 20 000 and EUR 100 000) set out in Article 319, paragraphs 1 or 2, respectively.

The same Article provides that, by way of derogation, competent authorities may grant a waiver from the requirement to calculate an annual operational risk loss to institutions with a business indicator that does not exceed EUR 1 billion, provided that the institution has demonstrated to the

satisfaction of the competent authority that it would be unduly burdensome for the institution to apply the first subparagraph.

The EBA identified that the challenges to the calculation of the annual operational risk loss are mostly due to the short timing available for the implementation of the appropriate systems and procedures, and the effort to put in place is not unduly burdensome when the institution is given an appropriate time span.

Institutions may temporarily report a business indicator equal to or higher than EUR 750 million due to transitory circumstances, and it would be unduly burdensome for these institutions to calculate the annual operational risk loss when exceeding the threshold is only a temporary exception within a certain time frame.

B. Policy objectives

Regarding the third deliverable, i.e. the one on specifying the conditions of 'unduly burdensome' for the calculation of the annual operational risk loss under Article 316(3) of Regulation (EU) 575/2013, the main operational objective is to identify, using data from the EBA's database of the mandatory Basel III exercise, the conditions that that would exceptionally waive the obligation of credit institution to calculation the past annual operational risk losses.

The current impact assessment focuses on identifying which would be the optimal period for an institution, belonging to the BI range of EUR 750 million and EUR 1 billion, to adjust to the anticipated changes and become able to keep track of the past losses.

To achieve this objective, the EBA based its analysis for the period 2015–2022 for a sample of 228 which participated in at least one of the reference dates within that period. The analysis will present results, not only static data, i.e. BI levels at point-in-time, but also dynamic data that refer to the transition of BIs amongst different BI buckets.

C. Examined options

Table 1 shows the allocation of banks into different BI buckets. The BI buckets were created to align with those inferred in the CRR3/CRD6 provisions, i.e. BI < EUR 750 million which corresponds to banks which are not required to report annual losses, BI > EUR 1 billion which corresponds to banks required to report past annual losses, and EUR 750 million < BI < EUR 1 billion, which include banks that under certain circumstances would be waived from reporting past annual losses.

The original sample comprises 228 that submitted data, at least once, for the Basel III monitoring exercise over the period 2015–2022 (see Table 1 and Table 2). 15 of 228 banks have not submitted any data for BI over the above period (see Table 2), while 213 have submitted BI data for at least once over the specified period. However, the banks consistently submitting data over the specified period drops to slightly above 100 banks. The sample of banks submitting BI data is stable over

2015–2017 at 138, while it gradually drops over 2018–2020. Due to the implementation of the EBA mandatory Basel III monitoring exercise from December 2021 reference date, the sample of BI submitting banks remains above 167 over 2021–2022 (see Table 1).

Table 1: Allocation of banks into Business Indicator buckets, number of banks

BI buckets	2015	2016	2017	2018	2019	2020	2021	2022
BI < 750 mn	62	61	62	47	48	46	80	74
750 mn < BI < 1 bn	13	12	10	9	5	5	11	12
BI > 1 bn	63	65	66	69	61	56	78	81
Total reporting banks	138	138	138	125	114	107	169	167
Non reporting	90	90	90	103	114	121	59	61
Total	228	228	228	228	228	228	228	228

Due to the adequacy and reliability of data, the basis for our analysis is the 2021–2022 period, where, except from the point-in time analysis, an analysis of the transitions among the buckets will be examined.

Regarding the point-in-time analysis, we observe that in 2021 there were 80 banks showing BIs less than EUR 750 million, 78 over EUR 1 billion, and 11 banks belonging in the range of EUR 750 million to EUR 1 billion; the EBA was mandated to examine the criteria according to which banks would be allowed to not report past annual losses. For 2022, the picture remains roughly the same, with the banks belonging to the range of EUR 750 million to EUR 1 billion increasing by one.

It is worth mentioning that almost all banks, even those that indicate BI less than EUR 750 million, report past annual losses, albeit the time series appear to be incomplete for some of the banks with BI less than EUR 750 million.

Another fact worth mentioning is that out of the 213 banks that reported BI data over the period 2015–2022, 147 moved among the buckets at least once, while 66 remained consistently at the same bucket. It is noteworthy that none of the banks remained consistently in the bucket that ranges from EUR 750 million to EUR 1 billion, which implies that there is no need to implement a provision for this subset of banks that would be of permanent nature (see Table 2).

Table 2: Number of banks that consistently been assigned to a BI bucket vs those which moved buckets over the examined period

BI buckets	Number of banks
(a) Banks consistently been assigned to the same BI bucket:	**66**
(a1) BI < 750 mn	23
(a2) 750 mn < BI < 1 bn	0
(a3) BI > 1 bn	43

(b) Banks consistently not reporting BI data over the examined period	**15**
(c) Banks that have moved among buckets at least once over the examined period	**147**
Total	**228**

Table 3 examines the transitions from one bucket to another from 2021 to 2022. Out of the 11 banks that belonged to the range-in-focus (henceforth 'RIF'), i.e. EUR 750 million to EUR 1 billion, in 2022 two moved to the lower bucket, two to the higher bucket while seven remained at the RIF. In addition, there was a bank that moved from the higher bucket to the RIF, while four other banks moved from the lower bucket to the RIF. Therefore, while the total number of banks belonging to the RIF, the composition of this subsample is much different. In a nutshell, 64% of the banks belonging in RIF remain at the same bucket when examining a short-term transition dynamic.

Table 3: Short-term (2021-2022) BI transition table

BI buckets	BI < 750 mn	750 mn < BI < 1 bn	BI > 1 bn	Non reporting	Total (2021)
BI < 750 mn	72	4	1	3	80
750 mn < BI < 1 bn	2	7	2	0	11
BI > 1 bn	0	1	77	0	78
Non reporting	0	0	1	58	59
Total (2022)	74	12	81	61	228

When examining the transition dynamics in medium-term (2019–2022), it seems that 40% of the examined banks remained at the RIF bucket, i.e. two of five banks that belonged to the RIF bucket in 2019 continue belonging to the same sample in 2022.

Table 4: Medium-term (2019–2022) BI transition table

BI buckets	BI < 750 mn	750 mn < BI < 1 bn	BI > 1 bn	Non reporting	Total (2019)
BI < 750 mn	29	3	1	15	48
750 mn < BI < 1 bn	1	2	0	2	5
BI > 1 bn	2	1	56	2	61
Non reporting	42	6	24	42	114
Total (2022)	74	12	81	61	228

Finally, when considering the longest transition period (2015–2022), 23% of the banks in the sample belonging to RIF bucket in 2015 remained at the same bucket in 2022.

Table 5: Longest-term (2015–2022) BI transition table

BI buckets	BI < 750 mn	750 mn < BI < 1 bn	BI > 1 bn	Non report-ing	Total (2015)
BI < 750 mn	29	3	1	29	62
750 mn < BI < 1 bn	3	3	3	4	13
BI > 1 bn	1	0	52	10	63
Non reporting	41	6	25	18	90
Total (2022)	74	12	81	61	228

The medium-term and longest-term transition tables (see Table 4, and Table 5) show a high number of transition percentages from the RIF bucket to the bucket of banks not reporting BI figures (40% and 31%, respectively), while in the short-term transition table (Table 3) the respective percentage is zero. This renders the short-term transition table more reliable in relation to the other two.

Moreover, there is a seemingly contradicting finding between item '(a2)' of Table 2 and the number of banks that remained at RIF bucket when comparing 2015 and 2022 (Table 5). The first examines whether the banks reported values, for every year between 2015 and 2022, that consistently belong to the RIF bucket, while the later compares only years 2015 and 2022. The fact that the latter shows that three banks remained at the same bucket means that these three banks moved out and then again in the RIF bucket over that period, but they did not remain in the RIF bucket over the entire period.

D. Cost-Benefit Analysis [for RTS on unduly burdensome]

As indicated by the EBA mandatory Basel III monitoring exercise data, most of the reporting banks, that exhibit BI less than EUR 750 million, already report past annual losses for the Exercise. Although, in some cases, the dataset in incomplete, i.e. less than the 10-year length, the most recent data show that all banks are in the position to calculate past data for the main two thresholds, i.e. 20 000 and 100 000 thresholds. The same applies for the banks that belong to the RIF bucket.

Thus, the overall additional cost of calculating annual past losses for banks that currently belong to the lower bucket or for those that will remain to the RIF bucket would be minimal, indicating that there is no need for waiving banks from this obligation on the basis of additional cost involved with this calculation.

However, on operational grounds, the EBA recognises the need for a temporary exclusion from the reporting requirements for banks that are either ***not able to temporarily calculate the annual past losses*** or ***they are expected to drop to the BI bucket that will permanently exclude them from the obligation of reporting past losses***.

To assess the period needed for such a waiver for banks belonging to the RIF bucket, the EBA examined the transitions to the bucket 'BI less than EUR 750 million'. The transition appears to be low, although not negligible (18% for the short-term to 31% for the longest term).

E. Preferred Option

Given the enhanced representativeness and adequacy of data referring to the 2021–2022 period, the 18% transition percentage (from RIF to the lowest bucket) is deemed as the most reliable. Considering this estimation, the EBA believes that one-year calendar period or four consecutive COREP reporting dates would be an adequate period for the waiver from reporting annual past losses.

4.4 Feedback on the public consultation

The EBA publicly consulted on the draft proposal contained in this paper.

The consultation period lasted for three months and ended on 6 September 2024. Nineteen responses were received, of which fourteen were published on the EBA website. The EBA also hosted a workshop with industry participants on 12 November 2024.

This paper presents a summary of the key points and other comments arising from the consultation, the analysis and discussion triggered by these comments and the actions taken to address them if deemed necessary.

In many cases several industry bodies made similar comments, or the same body repeated its comments in the response to different questions. In such cases, the comments, and EBA analysis are included in the section of this paper where EBA considers them most appropriate.

Changes to the draft RTS have been incorporated as a result of the responses received during the public consultation.

Summary of key issues and the EBA's response

RTS on establishing a risk taxonomy on operational risk

Feedback received during the public consultation and during the industry workshop held at the EBA premises on 12 November 2024 were supportive of the approach proposed by the EBA, in particular on the continuity with the Basel framework on event types and on the granularity of the categories. Comments received were very detailed and suggested enriched or alternative definitions of categories and attributes, as well as proposing new categories or attributes (or suggesting their merge or deletion). Furthermore, respondents encouraged further alignment with the SREP and DORA frameworks.

As a result, the draft final RTS pursues greater simplicity and features a reduced number of Level 2 categories and attributes, as well as enriched and more detailed descriptions.

Most comments were incorporated in the final draft RTS, and the main changes are the following:

— Alignment with DORA: 'ICT risk' is an attribute and institutions should ensure alignment with the ICT-related incidents reported under the Regulation (EU) 2022/2554. In particular, for the attribute 'ICT risk – Cyber', institutions should ensure consistency with the major ICT-related incidents reported as 'cybersecurity related' as per the Commission Implementing Regulation (EU) with regard to the standard forms, templates, and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat;

- ESG: two attributes have been retained, one on greenwashing risk and one that encompasses E, S, and G risks;
- Business disruption and business failures (BCM): the reference to BCM has been deleted, it covers several ETs. A stricter link to Basel definition has been pursued;
- Reference to intentionality: the intentionality is now taken into account only if it is objectively identifiable by the institution;
- Damage to physical assets: this event type has been enriched with two Level 2 categories (one for natural disasters and one for other external events);
- Business Disruption due to System Failures and Deficiencies: the difference between network, software and hardware failure is no longer disentangled. Furthermore, 'Business continuity' is an attribute, avoiding overlapping with other Level 2 categories;
- Execution, Delivery and Process Management: events involving third parties are now reported via a dedicated attribute.

RTS on specifying the condition of 'unduly burdensome'

While being supportive of the approach proposed by the EBA, some respondents argued that, in case of M&A where at least one of the institutions already calculated the annual operational risk loss before the M&A took place, the group may need more than one year to integrate the loss data set of the acquired entities. The EBA acknowledges the operational challenges faced by institutions that undergo an M&A process, and amended the draft RTS allowing for a waiver of two years from the calculation of the annual operational risk loss when at least one institution already calculated the annual operational risk loss before the M&A.

Regarding other cases when it would be unduly burdensome for an institution to calculate the annual operational risk loss, the feedback received were either not in scope of the draft RTS, or not in line with the CRR.

RTS on specifying how institutions shall determine the adjustments to their loss data set following the inclusion of losses from merged or acquired entities or activities

Comments received pointed to the difficulties of merging the loss dataset when the acquired entity or activities don't have such dataset, or when the quality of the dataset is not appropriate. The EBA acknowledges the issue and the draft RTS has been amended in order to expand the use of the proxy formula (i.e. the formula that the acquiring institution can use when it is not able to promptly include the losses from the acquired entity or activities in the loss dataset): when the acquired entity or activities do not have data on historical losses, or when their quality is not appropriate, because they are not required by law to build a loss dataset, then the acquiring entity can use the proxy formula provided in the draft RTS to cover the years for which there is no loss data, or their quality is not appropriate. Potentially, the proxy formula can be used to cover up to 10 years before

the acquisition of the entity or of the activities was finalised. For each year following the acquisition of the entity or of the activities, the acquiring entity should use the loss dataset which includes the losses of the acquiring entity or activities, thus phasing out the use of the proxy formula that should no longer be used after a maximum of 10 years.

Conversely, when the acquired entity of activities is required by law to build a loss dataset, the acquiring entity can use the proxy formula for up to two years, after which it is expected to have successfully integrated the losses of the acquired entity or activities into its loss dataset.

Summary of responses to the consultation and the EBA's analysis

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
General comments			
Loss threshold for the taxonomy	For one respondent, while the consultation paper proposes that the new taxonomy would be applicable to events with an impact of greater than EUR 20 000 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 taxonomy is independent of loss thresholds and may be used by banks also for losses below EUR 20 000.	No amendments
General features of the draft RTS	For one respondent 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).	The EBA acknowledges the issue, and this comment has been addressed by rearranging the Level 2 categories to be clearer between types of events.	RTS amended accordingly
Loss event timing	For one respondent, it should be clearly stated in the RTS that among the three main dates characterising an operational risk event (occurrence, detection, first accounting), the latter should be considered for identifying the 10-year layer of historical data on which it would be necessary to re-map to the new Level 1 and Level 2.	Article 317(3) of the CRR states that the accounting date is relevant for loss inclusion in the 10-year window.	No amendments

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Responses to questions in Consultation Paper EBA/CP/2024/13			
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.			
Internal fraud/Intentional mismarking	Some respondents ask for more clarity on where 'Rogue Trading' would be classified, noting that the scope of this L2 category may be too narrow.	The category intentional mismarking has been removed and mentioned as a way to manipulate or thefts data or commit rogue trading. Rogue trading has been explicitly added in both 'internal fraud committed against the institution' and 'internal fraud committed against other stakeholders'.	RTS amended accordingly
Internal fraud/Intentional fraud committed against the institution	One respondent notes that whilst External Fraud contains a category for the theft of data, this is omitted from Internal Fraud.	Data theft has been explicitly mentioned in the relevant categories of external fraud.	RTS amended accordingly
Internal fraud/Malicious physical damage to employees, institution's physical asset and public assets	For some respondents, whilst malicious physical damage to employees', institution's physical assets and public assets has been included, damage to virtual assets has been excluded.	This category has been removed. Damage to physical assets of any type is, by default, included in ET5. Where there is evidence that such a damage is due to malicious actions (i.e. a fraud), it should be assigned to ET1 or ET2, depending on whether the fraudster is internal or external to the bank.	RTS amended accordingly
Internal fraud/Intentional sanctions violation	It is suggested that Internal Fraud should include 'Intentional facilitation of tax avoidance'.	'Tax evasion' has been included in ET4, under the Financial Crime category. It includes events perpetrated in the interest of the bank and those in the interest of the clients. If there is clear evidence that the tax evasion is committed to consciously circumvent	RTS amended accordingly

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		the tax regulation (and not as a way to interpret it), the loss event should be considered as an Internal Fraud against other stakeholders and assigned to ET 1.3.	
External fraud/Cyber attacks	Some respondents note that cybersecurity losses are classified into two levels of Level 1 event types 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 may prove difficult, as it is always possible to determine which losses come from a system failure, and which are generated by a cyber-attack. This will also make comparability between entities difficult. A cyber risk attribute instead of the L2 category might be easier to implement and more helpful. It is unclear whether the definition includes Distributed Denial of Service (DDoS) attacks, as in these cyber-attacks the perpetrators do not gain access to an institution's systems.	L2 categories related to cyber-attack have been removed from L1 event type 'External fraud'. Instead, an attribute 'ICT risk related to cyber' is introduced which encompasses DDoS attacks.	RTS amended accordingly
External fraud / Data theft and manipulation	It is noted that while theft of data has been included in the taxonomy, the theft by third parties of physical assets has been excluded.	Theft of physical assets has been included in a new category in ET2.	RTS amended accordingly

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
External fraud /First- and third-party fraud	Some respondents are of the view that 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. In addition, it is not clear what is meant with second party fraud. It is furthermore asked whether a case when a fraudster modifies a client's data and as result steals funds from his account, should be assigned with this category or Data theft and manipulation.	The distinction between first, second- and third-party frauds has been removed from ET2. The new classification criterion is whether or not the external fraud has been committed by a client of the bank.	RTS amended accordingly
Clients, Products and Business Practices/Anti-trust – anti-competition	Some respondents ask the differences between Clients, Products & Business Practices – Anti-trust / anti-competition (#4.1) and 'Improper market practices…' (#4.4): there are examples associated with benchmark manipulation in which improper market practices have involved the formation of cartels, breaching anti-trust laws.	Both categories are merged into one.	RTS amended accordingly
Clients, Products and Business Practices / Client istreatment – failure to ulfil uties to ustomer	Some respondents note that a number of new items in Event Type 4 are a little unclear definitionally. For instance, 4.1 (Client istreatment / failure to Fulfil Duties to Customers) definition includes the con-	The description has been expanded to include also potential customers.	RTS amended accordingly

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	cept 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. It is also asked what the connection is between Client Mistreatment/Failure to Fulfil Duties to Customer (#4.2) and '… Inadequate/Improper Service to Clients after Sales …' (#4.10) and 'Client Account Management … Negligent Loss of Client … Assets' (#7.2). These three risks are potentially overlapping, and as a consequence the following case study would prove difficult to classify. In addition, Client Mistreatment/Failure to Fulfil Duties to Customer (#4.2) is similar to the point above, as this definition excludes discrimination against potential customers applying to open an account with an institution.	Level 2 categories in ET4 have been further streamlined to make it clearer where certain losses should be mapped.	
Clients, Products and Business Practices/Improper Market Practices, Product and Service Design or Licensing	Several feedback 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 their point of view, at least product design should have its own risk category. They also consider that category 7.5 (Improper distribution/Marketing) should be included in level 1 Clients category. Indeed 7.5 (Improper Distribution/marketing) seems to include improper direct marketing practices, which are potentially currently allocated to the Level 1 category ET4, since it might	The segregation of the categories under ET4 have been changed to reflect these comments. Operating without a license is now moved to a different category together with other breaches of statute and regulation. Improper distribution and marketing has been moved from ET7 to ET4.	RTS amended accordingly

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	overlap with the categories 'Client Mistreatment/Failure to Fulfil Duties to Customer' and 'Improper Market Practices, Product and Service Design or Licensing'. In case improper market practices should be classified into two new Level 2 categories, potential changes at Level 1 loss distribution could occur.		
Clients, Products and Business Practices/Rights – obligation Failures in Preparation Phase	Some respondents believe that the scope of category 4.5 (Rights/Obligation Failures in Preparation Phase) is not clear. In their view, more details are needed 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 Basel 7. Otherwise, the fact of having failures in contractual obligations is very broad and would overlap with many other risks.	Rights and obligation failures have been merged in ET7 since the segregation by preparation and execution phase was not helpful.	RTS amended accordingly
Clients, Products and Business Practices/Insider Trading on firm's account	From the feedback received, it's not clear whether 'Insider Trading on Firm's Account' includes case where the employee uses privileged information to benefit clients, or 'Insider Trading not on Institution's Account' includes an employee using insider information to trade for his personal account. It is also not clear whether Insider Trading on Firm's Account is not already covered by the category Internal Frauds.	Insider trading has been moved to ET1 Internal Fraud	RTS amended accordingly

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Clients, Products and Business Practices / Model – Methodology Design Error	Some comments point that the 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. Furthermore, improper market practices (#4.4) and Model/Methodology Design Error (#4.7) have significant overlapping. For Clients, Products and Business Practices (#4), the Level 1 risk definition references both clients and products. It does not, however, reference business practices. As a consequence, where in the taxonomy would an institution record compensation paid to its shareholders due to the prospectus for its own rights issue being misleading? Or where in the taxonomy would an institution record compensation for misleading investor updates? Or where in the taxonomy would an institution record a model/methodology design error which does not relate to either clients or products? It is recommended to – Expand the Level 1 risk definition of Clients, Products and Business Practices to include business practices. This would make the Level 1 risk definition consistent with the Level 2 risks, e.g. model / methodology design errors (#4.7), may then relate to neither clients nor products;	In the EBA view, model design and model implementation are generally handled by different entities of the bank and therefore it is preferable to keep these categories separate under ET4 and ET7. Amending the Level 1 event types would no longer allow for a 1:1 mapping to the Basel event types, which we deem to be important.	No amendments

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	− Expand the definition of Risk Reference 4.2 from customers to stakeholders, e.g. customers, shareholders, investors, and also society.		
Clients, Products & Business Practices / Accidental Money Laundering and Terrorism Financing	Some respondents is of the view that distinguishing between intentional and accidental breaches of money laundering or sanctions rules requires knowledge that risk managers likely will not have at the time of recording the event and potentially will never be able to judge. Although the Basel II event type taxonomy does have a notion of intentionality with the 'Intentional Mismarking of Positions' Level 3 event type under Internal Fraud/Unauthorised Activity, the proposed taxonomy takes this concept much further than concealing unauthorised trading activity Furthermore, the categories 'Accidental Sanctions Violations' and 'Accidental Money Laundering and Terrorism Financing' appear similar. Also, similar to the comments included in Internal Fraud, they see category 4.8 (Accidental Sanctions Violations) as already included in category 4.9 (Accidental Money Laundering and Terrorism Financing). For some respondents, this category seems misleading as it includes also fines for deficiencies on AML processes but with no occurrence of accidental flows related to AML. Furthermore, the risk taxonomy is key for managing operational risk in general, and not only for capturing or classifying losses, and they are concerned	The distinction between intentional and accidental has been removed from the taxonomy. The categories 'Intentional sanctions violation' and 'Intentional money laundering and terrorism financing' have been removed by ET1 and, by default, included in ET4, with some amendments. Where there is evidence that such events are due to a fraud, they should be assigned to ET1 or ET2, depending on whether the fraudster is internal or external to the bank.	RTS amended accordingly

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	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. Finally, they are concerned with some of the features of the proposed taxonomy, including the 'intentionality' of the event, since 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. They 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.		
Clients, Products and Business Practices / Accidental sanctions violations	Some respondents report that for Sanctions and Money Laundering Breaches, only a minority of its members make a distinction between 'accidental' and 'intentional' breaches. They have commented that they would only have information about intentionality very rarely. Some members would see an	The distinction between intentional and accidental has been removed from the taxonomy (see comment above).	RTS amended accordingly

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	intentional sanctions breach as an internal fraud against the firm. They also ask how it is possible to qualify the accidental nature in these two Levels 2 versus the Levels 2 of the Internal fraud type events which mention the intentional aspect. Respondents also ask for guidance on how to distinguish between intentional and unintentional violation of sanctions.		
Clients, Products and Business Practices / Sale Service Failure	A few respondents ask whether this category includes errors in the loan granting process and misselling. Also, the categories Improper Distribution/Marketing (#7.5) and Sales Service Failure (#4.10) need to be merged within Clients, Products and Business Practices (#4), as staff will struggle to differentiate between them.	ET 7.5 and 4.10 have been merged to a new ET4 category 'Improper distribution marketing, including sale service failure'.	RTS amended accordingly
Damage to Physical Assets	Some respondents ask how to combine common events across two data sets, such as pandemic, conduct, etc. In addition, further clarification is needed on the pandemic subject: especially whether pandemic topics are included or not in ET5 (DPA).	The EBA has introduced Level 2 categories for damage to physical assets and expanded the descriptive text to further clarify which losses should be mapped to this category (i.e. pandemic events should be mapped to ET 5.1).	RTS amended accordingly

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Business Disruption and System Failures / Inadequate Business Continuity Planning – Event Management	Respondents ask why a poorly designed business continuity plan should not be flagged as a governance risk.	Governance Risk does not refer to internal governance of the bank.	No amendments
Business Disruption and System Failures / Network Failure not Related to Management of Transactions	Clarity is also sought on the reason for dividing the categories into transaction and non-transaction events, and what will this distinction be used for.	The comment has been taken onboard.	RTS amended accordingly
Business Disruption and System Failures / Software Failure not Related to Management of Transactions	For some respondents, Business Disruption & Systems Failures (#6) makes no reference to the failure of 3rd and 4th parties that increasingly are providing to institutions Infrastructure and Software as a Service (IaaS and SaaS), such as cloud computing and cyber security software. This is a significant omission, given the technology strategies of many financial institutions. The Level 2 risk taxonomy needs to be future proofed, by increasing the level of granularity for Business Disruption and Systems Failure, as it is currently too low for a risk category that is rapidly increasing in significance, as a consequence of the digital revolution. The same is true for the risk of cyber-crime. It is recommended to expand Business Disruption and Systems Failures (#6) to reflect the failures of third and fourth parties. Furthermore, it is recommended to include the following additional Level 2 risk categories in Business Disruption and Systems Failure: – 6.5 Disruption to data and storage, e.g. both data quality and capacity;	The RTS has been amended so that it equally captures all failures in one category.	RTS amended accordingly

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	− 6.6 Disruption to external infrastructure, e.g. incompatible operating software; telecoms & internet; and utilities, such as power outages and also surges; and − 6.7 Disruption to 3rd and 4th party suppliers.		
Execution, Delivery and Process Management / Client Account Mismanagement	For a respondent, External Fraud – Compensation for stakeholder losses: Banks operating in the UK currently voluntarily reimburse customers for their losses arising from Authorised Push Payment (APP) frauds, and this will become mandatory in October 2024. In addition, the UK's new Economic Crime and Corporate Transparency Act creates a new 'failure to prevent fraud' offence. Recommendation: Include an additional Level 2 risk under External Fraud of 'compensation for stakeholder losses' as a result of fraud, 10 or alternatively expand the definition of client account management (#7.2) to make the '…negligent loss or damage to client assets' explicitly include losses arising from the 'failure to prevent fraud'.	The EBA believes that such a subcategory would not materially increase the level of detail sought for the taxonomy.	No amendments
Execution, Delivery and Process Management / IT Failures Related to Management of Transactions	A few respondents see no need to classify certain IT incidents in the Processes category, as all of them should be linked to System Failures.	The EBA shares this view.	RTS amended accordingly
Question 2. Do you perceive the attribute 'greenwashing risk' as an operational risk or as	Most respondents consider greenwashing as a factor that could impact the existing risk types: conduct, litigation or reputational risks; in some cases, it could result in operational risk events that must	The EBA takes note of the respondent observations, open to consider greenwashing risk within operational risk attributes. The EBA also acknowledges that	Examples are provided in the background and rationale section.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
a reputational risk event? Please elaborate.	be recognised within the operational risk event base, in particular for the part related to the economic consequences that could impact the institution (e.g. sanctions, litigations, complaints for example linked to mis-advising). It is also relevant to reputational risk as a consequence, in light of the possible impacts in terms of damage to the corporate image for which a quantification is difficult to obtain. The respondents ask EBA to further clarify the definitions of the attributes linked to transitional and greenwashing risk as well as the distinction among them.	clarifications are needed with regard to the distinction between greenwashing risk and transition risk.	
	For some respondents, greenwashing is not a risk in itself but should be considered as an aggravation/provoking factor of risk including operational and reputational risk. Greenwashing can be considered as a fact generating reputational risk and liability risk. In the latter case, there may be a consequence on operational risk, the liability risk being equivalent to legal risk. However, conduct situations related to green product and mis-selling can generate 'mis-selling green'. Those situations are the only Greenwashing Operational Risk. The respondent asks to make a clear distinction between Greenwashing not considered as an Operational Risk and Conduct situations.	The EBA takes note of the respondent observations, open to consider greenwashing risk within operational risk attributes.	Examples are provided in the background and rationale section.
Question 3. To which Level 1 event types and/or Level 2 cat-	Most respondents are of the view that 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:	The EBA takes note of the respondents' proposal of mapping greenwashing risk under different categories of Event Type 4 and Event Type 7 and to disregard the mapping of greenwashing to Internal Fraud ET.	Mandatory links between greenwashing attribute and Event types and Level 2

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
egories would you map green-washing losses? Please provide a rationale.	- **ET4** (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. - **ET7** (Execution, Delivery and Process Management): if greenwashing arises from an error in the bank's reporting/disclosure activity. Instead, respondents state that greenwashing losses should not be related to Internal Fraud ET, as it is suggested in the table of the EBA, arguing that the relation between AML and greenwashing as both risks processes and controls set up are not the same). Within the above Level 1 ET, they propose that flexibility should be given in applying the ESG/Greenwashing attributes across all L2 within those ET1, and would welcome clear regulatory guidance and confirmation that for ET1 only events/losses are to be attributed with ESG/Greenwashing, if they relate to an ESG/Sustainability-related process, communication/disclosure or activity. They also suggest that greenwashing could be relevant for ET4**,** Sale Service failure as greenwashing is always connected to a claim when materializing as an operational risk and the respective claim always contains a mis-selling/incorrect advice aspects.	The EBA proposes to leave banks flexibility in assigning greenwashing risk according to the Event types considered more relevant.	categories are removed.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	For one respondent, the introduction of certain flags for events relating to greenwashing and physical and transition risk is deemed useful, limitedly to those parts of their effects that fall under operational risk (where other parts pertain to strategic and reputational risk).	The EBA takes note.	Attributes related to Physical, Transition, Social and Governance Risk have been deleted and merged in a unique ESG attribute.
	For one respondent, greenwashing losses could be mapped under ET1 'Clients, Products and 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 as well as 'Client Mistreatment/Failure to Fulfil Duties to Customer', 'Rights/Obligation Failures in Preparation Phase', 'Sale Service Failure' and under ET7 'Execution, Delivery and Process Management' to Level 2 categories 'Rights/Obligation Failures in Execution Phase', 'Improper Distribution/Marketing' and 'Regulatory and Tax Authorities, including Reporting' since there can be 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 respondent proposes to eliminate the link of greenwashing risk with: 'Intentional Sanctions Violation', 'Intentional Money Laundering and Terrorism Financing'; 'Accidental Sanctions Violations', 'Accidental Money Laundering and Terrorism Financing'.	The EBA takes note of the respondent proposal of mapping greenwashing risk under different categories of Event Type 1 and Event Type 7 and to disregard the mapping of greenwashing to Intentional and Accidental Sanctions violation, Intentional and Accidental money laundering and terrorism financing. The EBA proposes to leave banks flexibility in assigning greenwashing risk according to the Event types considered more relevant.	Removed links between greenwashing attribute and Event types and Level 2 categories.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	For another respondent, greenwashing can lead to disputes with authorities, disputes with clients or disputes with third Parties and could be mapped as: 'Client Mistreatment/Failure to Fulfil Duties to Customer to Cover the Other Conduct Dimension'; 'Improper Market Practices, Product and Service Design or Licensing'; 'Rights/Obligation Failures in Preparation Phase'; 'Sale Service Failure To Cover the Green Mis-Selling'; 'Client Account Mismanagement'; 'Rights/Obligation Failures in Execution Phase'; 'Improper Distribution/Marketing'; 'Regulatory and Tax Authorities, including Reporting'.	The EBA takes note.	Attributes related to Physical, Transition, Social and Governance Risk have been deleted and merged in a unique ESG attribute.
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.	For several respondents 'Environmental risk' (both physical and transition) and broader ESG factors are drivers of existing traditional risks such as credit, market or operational risk. Respondents observe that transition risk is at an early stage but in the future fines, claims and customer complains might be linked to the EU sustainable finance legislative and regulatory framework. For these reasons it might be considered to flag an event in ET4 as linked to the bank's own transition risk. Respondents ask to clarify the definition of environmental risk, as some would consider transition risk under ET4 'Clients, Products and Business Practices' while others would consider it under ET7 'Execution, Delivery and Process Management'. The respondents point out that in the CP Annex there is no articulation in transition risk and physical risk as there is in the scheme in Section 20.	The EBA takes note of the respondents' proposal of mapping transition risk under different categories of Event Type 4 and Event Type 7. The EBA proposes to leave banks flexibility in assigning ESG attribute, now encompassing transition risk, according to the Event types and categories considered more relevant.	Transition risk attribute included under ESG attribute and increased flexibility in the mapping with L2 categories. Examples are provided in the background and rationale section.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	For some respondents, Transition Risk is a risk driver and not a proper operational risk event. They consider it as a non-financial risk that crosses different operational sub-risk types and can result in operational risk event materialising under the specific operational sub-risk type. The respondent highlights the following drivers: i) 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); ii) behavioural 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); iii) behavioural 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); iv) Technical developments can cause misconduct by a new technology or digitalisation (e.g. fundamental	The EBA acknowledges that implementing 5 different attributes for ESG related risks may be too much cumbersome at this stage. In light of simplification, the EBA proposes to adopt one ESG attribute and one greenwashing attribute.	Attributes related to Physical, transition, social and Governance risk have been deleted and merged in a single ESG attribute

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	right violation, product not meeting the needs of people with disabilities etc.) (social risk). The respondent observes that all these cases can fall into other risks (governance, social etc.). However, 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, the respondent proposes to map transition risk to ET1 'Execution, Delivery and Process Management' and Level 2 category 'Regulatory and Tax Authorities, including Reporting'. Additionally, the respondent asks to the EBA to define clearly and accurately what is considered transition risk and what is social and governance risk so that there are no interpretations and entities can classify their losses following homogeneous criteria.		
	For one respondent the direct impact of an ESG risk in operational risk category is difficult to identify and assess unless it is a physical ESG risks that would have consequences on business continuity or on value of the bank assets. The respondent would consider transition risk as an operational risk only in specific cases of claims or summonses from clients or authorities for non-compliance with ESG standards.	The EBA takes note.	Attributes related to Physical, transition, social and Governance risk have been deleted and merged in a single ESG attribute
	For some respondents, environmental risk and broader ESG factors are primarily drivers of existing traditional risks such as market risk or credit risk,	The EBA acknowledges that implementing 5 different attributes for ESG related risks may be too much cumbersome at this stage. In light of simplification, the	Environmental, Social and Governance Risk merged into a

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	thus large parts of what constitutes transition risks are already covered by other risk categories. These factors can however lead to operational risk, if there is a penalty. However, the respondent disagrees with the introduction of an independent 'Greenwashing Risk' attribute, not defined by CRR 3. The respondent disagrees with the split of 5 ESG attributes, also in light of the fact that the CP associates them to few or none risk categories and claims that this split will lead to practical difficulties. The respondent asks to clarify the attributes definition and to provide examples to make the distinction more comprehensible. The respondent observes that 'Greenwashing Risk' should be considered part of 'transition risk' and could be mapped to different Level 2 categories: 'Processing/Execution Failures' under ET1 Execution, Delivery and Process Management; 'Improper Market Practices, Product and Service Design or Licensing' under ET1 Clients, Products and Business Practices; 'Inadequate Employment Practice'.	EBA proposes to adopt one ESG attribute and one greenwashing attribute. The EBA will provide in the Annex some examples to help banks in assigning the ESG and greenwashing attributes.	single attribute. Examples are provided in the background and rationale section
Question 5. Which of these attributes do you think would be the most difficult to identify? Please elaborate.			
ESG attributes	Some respondents ask for the purpose of having 5 flags related to ESG which are incompatible with most risk types. Due to the current status of ESG risk management practices, and the lack of industry	The EBA acknowledges that implementing 5 different attributes for ESG related risks may be too much cumbersome at this stage. In light of simplification, the EBA proposes to adopt one ESG attribute and one	Environmental, Social and Governance Risk merged into a

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	data, the respondent state that having only one flag related to ESG would suffice at this moment. Banks could voluntarily identify the five flags as subsets, but only the overall ESG risk flag should be mandatory, or also the Greenwashing flag at the most. Several respondents argue that the definitional boundaries of some attributes are not clear, especially the distinction between 'Greenwashing Risk' and 'Transition Risk'. Due to the current status of ESG risk management practices, and the lack of industry data, further clarification on the definition and specific examples provided by the EBA are deemed significantly helpful.	greenwashing attribute. The EBA will provide in the Annex some examples to help banks in assigning the ESG and greenwashing attributes.	unique attribute. Examples are provided in the background and rationale section
Physical Risk	Some respondents argue that physical risk is among the most difficult flags since it is not possible to distinguish if a natural disaster (like heavy rain, hailstorm, flood etc.) is due to climate change or not.	The EBA acknowledges that attributing specific natural disasters directly to climate change could be a challenging task. While it is difficult to definitively state that an individual event is caused by climate change, climate change is increasing the frequency and intensity of extreme weather events. So, the broader trend of changing weather patterns could more and more be considered when evaluating this attribute.	No amendments
Physical Risk, Social, Governance, Greenwashing	For other respondents, except for physical risks that correspond to the risk of Damage to Physical Assets, manual event-by-event identification is required for ESG attributes, making impossible the automation of the flag in the database.	The EBA acknowledges that there might be difficulties in automatically identifying new risks/factors. However, the EBA observes that CRR 3 explicitly requires to report information on ESG.	No amendments

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Governance, Social, Transition Risk	From the feedback received, there are difficulties in the precise classification of governance and social risks and transition Risk. The events under the Governance attribute 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. Furthermore, the scope of the Social Risk attribute is not sufficiently clear and too broad.	The EBA will provide in the Annex some examples to help banks in assigning the ESG and greenwashing attributes.	Examples are provided in the background and rationale section
Legal Risk	For most respondents, clarification regarding the 'Legal Risk – Misconduct' flag is deemed extremely useful: indeed, the consultation paper refers to the CRR definition of legal risk (i.e. 'legal risk' refers to losses, including expenses, fines, penalties or punitive damages, caused by events that result in legal proceedings) but it is not clear whether legal proceedings also include complaints and other kinds of reimbursements not stemming from lawsuits. Furthermore, 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 adapta-	The EBA recognises the need to clarify the definition of loss events pertaining to legal risk. Loss events due to legal proceedings should encompass all legal disputes and settlements, including both mandated court settlements and out of court disputes and settlements. The EBA acknowledges that the transition to the new taxonomy, including the new attributes, may create costs. However, these costs would be only temporary until the new structure is integrated.	Definition amended (see Article 1, Paragraph 4)

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	tion of the new approach to risks, which will not correspond to an improvement in operational risk management.		
Pending Losses	Most respondents ask how to deal with pending losses when there are recoveries. For instance, material Pending losses are not common. If an item booked to a suspense account is confirmed to be an operational risk loss it would be treated the same as any other event. It would be challenging to identify all pending losses within the organisation that relate to an operational risk event. A pending loss is not an attribute (it is a temporary situation), and therefore a pending loss may be reported one quarter and then removed from the loss dataset next quarter if the event is resolved (e.g. in the case of a rapid recovery over a reporting quarter-end, where the discrepancy is initially posted to a suspense account). However, for other respondents, pending losses are temporary and can't be a stable taxonomy element to qualify a risk event. The exercise is theoretical 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. In addition, pending losses are not considered as losses as long as they have not been provisioned. Cash/security breaks have a dedicated process to make sure that they are correctly monitored according to their amount and their age. In our opinion, pending losses should not be reported as losses but could be reported via KRI.	The EBA acknowledges the issue, and the pending losses flag has been removed.	RTS amended accordingly

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Credit Risk Boundary (those not included in RWA on credit risk)	Some respondents state that, based on the current definition, credit risk is the only broader type where collected operational risk cases with credit risk impact can be excluded out of the capital calculation. The credit risk flag has to be ticked whenever out of an operational risk event a loan loss provision or credit risk exposure (RWAs) is generated. Boundary CR related events were collected and reported to Senior Management for respective action taking. Furthermore, clarification is needed if now under credit risk boundary should be considered only pure operational risk cases (cases included in credit risk RWA not to be considered under CR boundary). How this differs to pure operational risk events. How to flag those events which have operational risk root cause and bookings under credit risk RWA. Usually, banks have a product catalogue within their loss data collection. This boundary definition would even cause more complexity.	The EBA believes that Article 317(5) CRR is clear enough.	No amendments
Third-Party Risk	Most feedback note that the concept 'Third-Party' is not consistent across the document: - Third-party risk is defined as 'Losses that may arise for an institution in relation to its use of services provided by third-party service providers or by subcontractors of the latter, including through outsourcing arrangements'. - But one of the mandatory mappings is to Third-Party fraud that is defined as 'Fraudulent acts … that	The EBA acknowledges that this may create confusion as 'third-party' generally refers to third-party service providers or subcontractors, including outsourcing arrangements. L2 event type related to 'Third-Party Fraud' has been removed from L1 event category 'External Fraud'. Furthermore, labels of L2 event types regarding fraudulent acts related or not related to data theft or manipulation, are amended to avoid confusion with third-party service providers.	RTS amended accordingly

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	have been committed by means of the identity of another ignorant person'. - Using the identity of another person to commit fraud doesn´t mean that this person is a service provider or subcontractor. - Fraud committed by a third party is not an issue that is included as part of the standards and regulations of third-party risk management.		
Retail (including Banking and Retail brokerage)	Some respondents are of the view that losses applied to business lines may not be mutually exclusive and collectively exhaustive (MECE). There are losses events applying to different business lines.	If a loss event applies to different business lines, several flags could be used. The sentences stating that business lines attributes are MECE have been removed from the background and rationale section and from the recitals.	RTS amended accordingly
ICT Risk	For some respondents, cyber events are only included in the proposed taxonomy as a subset of Fraud, separate from Data Management, which means that events relating to cyber data theft may not be all easily reported. One way of addressing this may be the addition of a 'Cyber' attribute. For other respondents, 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.	L2 category related to cyber-attack is removed from L1 event type 'External Fraud'. Instead, two attributes are introduced, one on 'ICT Risk Related to Cyber' and one on 'ICT Risk not Related to Cyber'. This may ease the use of such attributes in banks database.	RTS amended accordingly

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	Most feedback seeks consistency with DORA.	ICT risk was removed from the L2 categories and included as two different attributes, with definitions linked to DORA.	RTS amended accordingly
Question 6. Do you agree with the inclusion of the attribute 'Large Loss Event'? If not, please elaborate.			
	For some respondents, it is not clear for which period large losses are to be determined (on a quarterly or annual basis). The labelling could only be temporary for some loss events, as larger losses may have been added over time.	The EBA shares this view: the volatility of the attributes contrasts with the nature of a taxonomy which is stability	Attribute 'Large Loss Event' and 'Ten largest Loss Events' deleted
	Most respondents don't agree with the introduction of the 'Large Loss Event' attribute as it is seen as a duplication of the reporting requirements and difficult to implement due to the need to constantly monitor and update this attribute.	The EBA acknowledges that the information is better captured in COREP due to the nature of the attribute. The monitoring and updating due to the volatility of the quantitative dimensions of the attribute would be rather burdensome.	Attribute 'Large Loss Event' and 'Ten Largest Loss Events' deleted
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.			

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Legal Risk – Misconduct	For most respondents, clarification regarding the 'Legal risk - Misconduct' flag is deemed useful: indeed, the consultation paper refers to the CRR definition of Legal Risk (i.e. 'Legal Risk' means losses, including expenses, fines, penalties or punitive damages, caused by events that result in legal proceedings), but it is not clear if legal proceedings include also complaints and other kind of reimbursements not following lawsuits. If only lawsuits are intended to be considered as legal proceedings, it would not be possible to flag as Misconduct related a potentially significant part of the operational risk database, thus making such an attribute somehow less useful.	The EBA acknowledges the need to clarify the definition of loss events pertaining to legal risk. Loss events due to legal proceedings should encompass all legal disputes and settlements, including both mandated court settlements and out of court disputes and settlements.	RTS amended accordingly
Legal risk – Other than Misconduct	For some respondents, it is not clear (1) why AML may be assigned to 'Legal Risk Other than Conduct' while 'Sanctions' doesn't. (2) Furthermore, the definition of the attribute that should exclude conduct topic includes 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'. They believe that this attribute should be clarified as to whether conduct events are included or not.	(1) The EBA acknowledges the issue. Both AML and sanctions are moved to the ET 4 'Clients, Products and Business Practices' and placed in the same L2 category of 'Financial Crime' (4.5). Loss events in 4.5 are assigned the attribute 'Legal Risk – Misconduct'. (2) As for the definition of 'Legal risk – Misconduct/Not Related to Misconduct' the RTS follows the Level 1 text, i.e. Recital (52a) of the CRR.	On (1), the RTS has been amended accordingly. On (2), the RTS has not been amended.
ICT Risk	For most respondents, the ICT attribute definition refers to security (malicious aspect) and not safety (human error; for instance, the use of network and	The definition of the ICT risk attribute is aligned with Article 4(52c) of the CRR and does refer not only to	RTS amended accordingly

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	information system). This seems to be restrictive and will be difficult to implement without clarifications. Furthermore, a cyber risk attribute might prove helpful as well.	ICT security. As per EBA Guidelines on ICT risk assessment under the SREP (EBA/GL/2017/05), ICT risk encompasses: ICT availability and continuity risk, ICT security risk, ICT change risk, ICT data integrity risk and ICT third-party risk, including ICT outsourcing risk. Furthermore, to better identify cyber risk, the final RTS introduced a 'ICT risk Related to Cyber' attribute and a 'ICT risk not related to cyber' attribute.	
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?	For some respondents, it is not clear how banks are requested to identify the events related to previous ten/three years in order to identify the perimeter of events to be re-mapped (namely, an event registered more than ten/three years ago could be still open if it refers to a legal case not already closed and therefore should be re-mapped to the new taxonomy even if it dates back to more than ten/three years). The final RTS should consider the first accounting date in order to identify events related to previous ten/three years. Also, the request to apply this new regulation to losses above EUR 20 000 threshold doesn't seem to be applicable because an event could remain under such a threshold for a certain period of time and then increase above EUR 20 000 and it should be therefore re-classified according to the new taxonomy.	Since the Level 1 event types have not changed from Basel, the EBA deems appropriate to map ten years back since there is no change to the current regime. The EBA also acknowledges that going back three years on the Level 2 categories or attributes would be too burdensome. The mapping may be performed on a voluntary basis. As a helper, the background and rationale section now includes a mapping from the taxonomy to the Basel taxonomy.	Included a mapping table to the Basel taxonomy
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 –	All respondents deem the length of the waivers as appropriate. One respondent argues that one year may not be enough to integrate the loss data set of the acquired entities even if one or more institu-	The EBA acknowledges that, following a M&A, the integration of the data set of the merged entities requires a significant effort, including where one or	The RTS is amended to allow a waiver of two years

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
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.	tions of the group already calculate the annual operational risk loss, and two years may be more appropriate.	more institutions of the group already calculate the annual operational risk loss.	
Question 10. Are there other cases where it should be considered to be unduly burdensome for institutions to calculate the annual operational risk loss?	One respondent argues that the draft RTS should provide a waiver when the institution, following a M&A, has a BI higher that EUR 1 billion, but the acquired or merged entities are not able to provide data on past losses of acceptable quality	The scope of the draft RTS encompasses only institutions whose BI is between EUR 750 million and EUR 1 billion.	No amendments
	One respondent commented that a waiver should be provided when an institution acquires an asset (e.g. a loan portfolio) and no data on past losses is available.	The EBA acknowledges the issue and the issue is addressed in the RTS for the adjustment of loss data sets following an M&A under Article 321(2) of the CRR.	No amendments
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.			
Different currencies of merging entities	For most respondents, in case of different currency used by merged or acquired entity from the currency of the acquiring institution, the exchange rate	According to the FAQ of the BCBS on OPE25.18, the foreign exchange rate to be used is the one at the time of the accounting of the loss.	No amendments

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	to be used for reporting purposes should be dependent on the instructions for such reporting template and it cannot be assumed that the exchange rate of the end of the period will be the one to be used. 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.		
Use of the proxy formula	For most respondents, 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. Such adaptation would not be automatic and would need to be performed on event-by-event basis with a lot of manual work required. The effort to build a loss data set should be applicable to operational losses starting from the data of merge or acquisition and at least two years should be allowed for this. The proposed proxy will be used for the purposes of calculation of the annual operational risk losses.	The EBA acknowledges the issue, thus the draft RTS is amended in order to allow the use of the proxy formula up to 10 years in the past when the acquired entity or activities were not required by law to set up a loss dataset. For each subsequent year, the acquiring company should use the annual operational risk loss determined by the loss dataset, thus phasing out the use of the proxy formula within 10 years.	RTS amended accordingly
Difficulties to merge databases using the EBA risk taxonomy	For one respondent, 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 EBA acknowledges the issue, thus the draft RTS is amended in order to allow the use of the proxy formula for up to 10 years in the past. For each subsequent year, the acquiring company should use the an-	RTS amended accordingly

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	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. For another respondent, any combined reporting after a merger would be most difficult to implement if the entity being merged with does not have good quality loss data for the required time period. Specific additional challenges reported include: • Data migration challenges. • Adjusting loss data set due to differences in currency between the acquired and acquiring institution. • Adjusting the loss data set due to differences in event taxonomy pre-merger. • Pre-merger loss threshold differences. • Article 318 requirements on the calculation of net and gross loss are exceedingly detailed and specific to implement and comply with confidence to the risk event dataset of a merged or acquired entity. • Combining common events across the two data sets, such as pandemic, widespread conduct events etc.	nual operational risk loss determined by the loss dataset, thus phasing out the use of the proxy formula within 10 years.	
Question 12. In your experience, would the provisions of			

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
this article apply to most mergers and acquisitions, or would data usually be promptly implemented in the loss data set of the reporting institution?			
Length of the use of the proxy formula	For most respondents, the one-year period to integrate and adjust the losses from merges or acquired entities or activities is too short given the heavy workload required to map historical internal loss data to event type and of historical data resumptions. Depending on the size/materiality of the acquired entity in comparison with the absorbing entity the delay could be longer/shorter. They consider that a two-year period should be allowed for.	The EBA acknowledges the issue, thus the draft RTS is amended in order to allow the use of the proxy formula for up to 10 years in the past. For each subsequent year, the acquiring company should use the annual operational risk loss determined by the loss dataset, thus phasing out the use of the proxy formula within 10 years.	RTS amended accordingly
Challenges of integrating the loss data sets	For one respondent, if the acquired company has previously maintained a loss database that includes a categorisation according to the previous methodology or according to the methodology of the CRR 3, the integration of a loss dataset can be completed more quickly and easily than if no such categorisation exists. The further the requirements for the data set are expanded or extended (e.g., now through the attributes), the more complex the migration of the loss dataset becomes. This applies in particular to the loss dataset of subsidiaries that are not financial institutions. For another respondent, the ability of a firm to implement the provisions of the article depends on	The EBA acknowledges the issue, thus the draft RTS is amended in order to allow the use of the proxy formula for up to 10 years in the past. For each subsequent year, the acquiring company should use the annual operational risk loss determined by the loss dataset, thus phasing out the use of the proxy formula within 10 years.	Draft RTS amended accordingly

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	the acquired entity already having in place a loss data collection process aligned with the new proposed EBA event type and risk taxonomies. If the acquired entity did not have this data, the collection of ALL the requested attributes could require material effort to be put in place on a retroactive base.		
Question 13. Are there other adjustments that should be considered in these draft RTS? If yes, please elaborate.	Comments reported under this question were moved to the most appropriate question in the table.		