
DRAFT RTS ON THE OPERATIONAL RISK MANAGEMENT FRAMEWORK

PUBLIC HEARING · 29 SEPTEMBER 2026

EBA/CP/2026/18 · MANDATE UNDER ARTICLE 323 OF REGULATION (EU) 575/2013



Guidance for participants

- Please note that **microphones are muted** on entry. Kindly keep yourself muted during the presentation.
- Do **not** switch on your **camera** if you are not the speaker. To increase audio quality please turn off video streaming.
- If you would like to intervene during the **Q&A session**, please write your question(s) directly in the Teams chat.
- In case of **technical issues** with Teams:
 - ☐ Log out and log in again.
 - ☐ If that still does not solve your issue, you can try dialing in via phone through one of the local access numbers provided in the invitation or send an email to: meetings@eba.europa.eu

Contents

1 Objectives of this public hearing

2 The mandate and its value

3 Background and policy context

4 The operational risk management framework

5 Governance, process, assessment and use test

6 Data, taxonomy, proportionality and simplicity

7 ICT, reporting, validation and audit

8 Impact assessment and next steps

Structure of the draft RTS — 15 articles in four chapters

I

General provisions

Arts 1–3 · scope, integration with ICT risk management, definitions

II

Operational risk management framework

Arts 4–9 · establishment, documentation, process, assessment system, use test, data and taxonomy

III

Governance

Art 10 · independent operational risk management function

IV

Reporting, validation and audit

Arts 11–15 · reporting, compliance and validation, audit, data flows

Objectives of this public hearing

- Present the draft regulatory technical standards on institutions' arrangements for managing operational risk (EBA/CP/2026/18, published on 26 August 2026).
- Explain the policy rationale, the structure of the proposed framework and the proportionality approach applied throughout the draft RTS.
- Highlight the areas on which the EBA is seeking evidence, in particular internal loss recording thresholds and the metrics used to set operational risk appetite.
- Collect early feedback from stakeholders. This public hearing does not replace written responses to the consultation.
- Comments should be submitted through the EBA consultation page by 31 December 2026.



The mandate — Article 323 CRR and its value

Article 323(1) CRR — institutions must have in place

- (a) a well-documented operational risk assessment and management system, closely integrated into day-to-day risk management processes;
- (b) an operational risk management function independent from business and operational units;
- (c) a system of reporting to senior management;
- (d) regular monitoring and reporting of exposures and loss experience, with corrective actions;
- (e) routines for ensuring compliance and policies for the treatment of non-compliance;
- (f) regular reviews by internal or external auditors;
- (g) internal validation processes that operate in a sound and effective manner;
- (h) transparent and accessible data flows and processes for the assessment system.

Article 323(2) CRR — the EBA mandate

Draft RTS specifying points (a) to (h), taking into account the size and complexity of the institution; applicable to all institutions subject to the CRR, individually and, where applicable, on a consolidated and sub-consolidated basis.

Why the mandate matters

1

Prudential needs

CRR3 replaced internal models with a single standardised approach, but sound operational risk management remains essential to the safety and soundness of institutions. The RTS extend to all institutions, in a proportionate manner, the management disciplines previously expected mainly of AMA users.

2

Resilience

A sound framework underpins the ability to deliver critical or important functions through disruption — from ICT incidents and third-party failures to emerging risks such as ESG factors, new technologies and geopolitical developments.

3

A common Union baseline

Harmonised minimum requirements and more consistent supervisory expectations across the Union, applied proportionately and coherently with DORA and existing EBA Guidelines.

Background and policy context

- CRR3 (Regulation (EU) 2024/1623) replaced the previous approaches, including the advanced measurement approaches, with a single standardised approach for own funds requirements.
- Greater comparability and simplicity for Pillar 1 do not reduce the need for sound arrangements to identify, assess, monitor, control, mitigate and report operational risk.
- Supervisory experience gained under the advanced measurement approaches remains relevant: strong governance, robust internal loss data, sound scenario-based assessment and effective independent challenge.

Main references the draft RTS build on

Basel Committee

Principles for the Sound Management of Operational Risk (2021)

Basel Committee

Principles for Operational Resilience and BCBS 239

Delegated Regulation (EU) 2018/959

RTS on the assessment methodology for the AMA

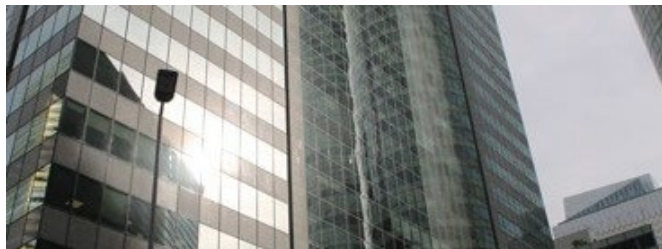
EBA Guidelines

Internal governance, third-party risk and ESG risks (EBA/GL/2025/01)

DORA

Regulation (EU) 2022/2554 and related technical standards

The OpRisk Management Framework: three interrelated components



Governance

Responsibilities of the management body, senior management and internal control functions, including the independent operational risk management function.



Management process

The policies, processes and procedures used to identify, monitor, control, mitigate and report operational risk, embedded in the institution's day-to-day operations.



Assessment system

The methods, data, taxonomy, indicators and analyses supporting the assessment of the operational risk profile.

The three components are mutually reinforcing and operate as an integrated whole within the institution's broader governance, risk management and operational resilience arrangements.



Question 2 Are the proposed definitions of the operational risk management framework, operational risk profile and operational risk appetite sufficiently clear and aligned with Article 4(1), point (52a), and Article 323 CRR? Would any additional definitions be necessary?

Governance — management body and senior management

Management body — supervisory function

Approves the framework; defines and approves the operational risk appetite at least annually; monitors continuously that the risk profile stays within appetite.

Management body — management function

Responsible for implementing the approved framework.

The framework — Article 4

Documented, institution-wide, integrated into overall risk management and day-to-day operations, and reinforcing the operational resilience approach. Effectiveness evaluated at least annually (business indicator $\geq$ EUR 750 million) or every two years.

Senior management

Implements the policies, processes, procedures and systems; translates appetite into quantitative limits, such as loss-based limits, and monitors exposures, with escalation of breaches.

Business indicator below EUR 750 million

The business indicator, or its relevant components, may be the only proxy for appetite; the competent authority may require additional quantitative measures.

Documentation — Article 5

Complete, consistent, accurate, up to date, approved and securely retained; detailed enough for independent review, including by competent authorities.



Questions 3 and 4 Do respondents agree with the proposed responsibilities of the management body and senior management, and with the use of the business indicator, or its relevant components, as a proxy for operational risk appetite below EUR 750 million? What are the views on the use of past operational risk losses, and which other measures, indicators or limits are used to set risk appetite? Are the documentation requirements appropriate and proportionate?

The independent operational risk management function

- Second line of defence: performs its tasks independently of the business and operational units it oversees, with no responsibility for their day-to-day management, operation or control performance.
- Designs, develops, maintains and oversees the management process and the assessment system; reviews and contributes to the monitoring and reporting of the risk profile.
- Challenges the operational risk of new or materially changed products, markets, lines of business, processes and systems; oversees activities that could breach the risk appetite.
- Promotes a risk management culture through training and targets for loss prevention and reduction; not responsible for the audit function; cooperates with compliance, in particular on legal risk.
- Adequate resources, authority and stature, with support from the management body and senior management, and an institution-wide view where other functions oversee specific risks.
- **Head of the function:** appropriate expertise, regular and direct communication with the management body, active role in setting risk appetite and mitigation strategy, independence from the units overseen.



Question 12 Do respondents agree with the proposed tasks, authority, stature and resource requirements for the independent operational risk management function? Is the meaning of independence sufficiently clear and proportionate? How would institutions position the function within the second line of defence, in relation to other control functions such as risk management or compliance?

The operational risk management process

Article 6

?

Question 5

Do respondents agree with the proposed requirements for the operational risk management process, including the communication of operational risk information to the first line of defence and to staff responsible for the activities that give rise to operational risk? Is further clarification needed on Article 6(3), in particular as regards the scope, recipients and frequency of such communication?



1

Policies and procedures — established and maintained as part of the operational risk management framework.



2

Ongoing process — to identify, monitor, control, mitigate and report operational risk.



3

Clear ownership — the staff responsible for each component of the process are clearly identified.



4

Communication — results reach the first line of defence and those managing the activities that give rise to operational risk.



5

Risk culture — staff engagement and awareness of exposures and of the policies, processes and procedures.



6

Control activities — preventive, detective and corrective measures keeping exposures within operational risk limits.

The operational risk assessment system

- Includes the calculation of the business indicator component for all institutions and, where the business indicator is at least EUR 750 million, of the annual operational risk loss.
- Identifies and assesses operational risks through both a bottom-up and a top-down approach, so that exposures are managed within limits and, ultimately, within appetite.
- Detects and accurately categorises events, including where operational risk is intertwined with other risks such as ESG risk, and analyses their drivers and root causes.
- Applies assessment procedures proportionate to the risk profile: business process mapping, risk and control assessments, and scenario analysis and stress testing.
- Scenario analysis and stress testing support the internal capital adequacy assessment, the setting of appetite and limits, and the operational resilience approach — they are not intended to recreate internal models for Pillar 1.



Question 6 Do respondents agree with the proposed requirements for the operational risk assessment system, including business process mapping, risk and control assessments, scenario analysis and stress testing? Are these requirements sufficiently proportionate for institutions with different operational risk profiles?

The use test

Article 8 — integration into day-to-day operations and decision-making

Gives concrete effect to the management process (Article 6) and the assessment system (Article 7) presented in the previous slides.

?

Question 7

Do respondents agree with the proposed requirements for embedding the operational risk management framework in day-to-day operations and decision-making, including in relation to approval of products, activities, systems and processes, action plans, business and insurance plans and change management?

1



Embedded everywhere

— used to manage operational risk across business areas, units and legal entities.

2



Continuous development

— regularly updated as the institution gains experience and sophistication.

3



Clear communication

— of risk appetite, objectives and the link with business strategy and product approval.

4



Event protocols

— predetermined protocols to identify, analyse, manage and report events end to end.

5



Relevant, timely information

— inputs reflect the business model and risk profile; outputs reach decision-makers.

6



Outputs drive decisions

— action plans, business and insurance plans, change management and continuous improvement.

Operational risk data, information and taxonomy

Data to be collected — Article 9(1)–(3)

All institutions: processes to collect, record, store, aggregate, analyse and monitor operational risk data, and to monitor internal and external factors.

Business indicator $\geq$ EUR 750 million

Relevant losses below EUR 20,000 (criteria defined internally), incidents, near misses and boundary cases, root-cause fields, external loss data, scenario and stress-testing results, risk and control assessments, key risk and control indicators.

Business indicator $<$ EUR 750 million

All losses above EUR 20,000 plus relevant and material losses below that threshold, together with a subset of the other elements.

From a loss taxonomy to an event taxonomy — Article 9(5)–(7)

The taxonomy no longer serves only to classify losses as defined under CRR3: it must enable the consistent identification and classification of operational risk events and the aggregation of the risk profile across business processes and organisational levels. Consistency with the Article 317(9) CRR and with the applicable technical standards on operational risk loss data classification taxonomy is required at or above EUR 750 million and encouraged below.

Boundary cases clarified for Pillar 1 and Pillar 2 — Article 9(2)(b)

Pillar 1 risks (credit, counterparty and CVA risk): losses stay classified under those risks but are captured in the operational risk data; market risk losses already fall within operational risk (Article 317(6) CRR). Pillar 2 risks (strategic, business, liquidity risk): always treated as operational risk, contributing to operational risk own funds requirements and, where the business indicator is $\geq$ EUR 750 million, to the annual operational risk loss.



Questions 8–11 Should the concept of “relevance” for losses below EUR 20,000 be further developed (Q8)? Below EUR 750 million, is the proposed loss data threshold proportionate, and should “relevance and materiality” be further developed (Q9)? Should taxonomy consistency with Article 317(9) CRR be required above EUR 750 million and only recommended below (Q10)? Do respondents agree with the interpretation of boundary cases with Pillar 1 and Pillar 2 risks (Q11)?

Proportionality and simplicity

	Business indicator below EUR 750 million	Business indicator at or above EUR 750 million
Framework effectiveness review	At least every two years	At least annually
Operational risk appetite	Business indicator, or its relevant components, may be the only proxy	Quantitative limits, with exposures monitored against them
Operational risk data	Reduced set: relevant and material losses below EUR 20,000	Extended set: relevant losses below EUR 20,000, near misses, scenario and stress-testing results, key risk and control indicators
Operational risk taxonomy	Consistency with the RTS on operational risk taxonomy recommended	Consistency with the RTS on operational risk taxonomy required
Reporting to the management body	At least annually	At least quarterly

Simplicity by design — *requirements kept as simple as prudential needs allow*

One existing metric

The business indicator already calculated under Article 314 CRR sets the threshold: no new classification, no supervisory discretion.

Principle-based

Harmonised minimum obligations; simpler arrangements allowed where they remain effective.

Built on existing frameworks

Reliance on DORA arrangements, EBA Guidelines and the RTS on taxonomy.

No new capital model

Tools serve risk management and the ICAAP; no change to own funds requirements; costs mostly one-off.



Question 16 Is the differentiation based on the EUR 750 million business indicator threshold appropriate, or should different but equally simple and consistent metrics be introduced? Is proportionality sufficiently reflected throughout the draft RTS?

Integration with ICT risk management

- ICT risk management, as required by DORA (Regulation (EU) 2022/2554) and Directive (EU) 2022/2556, forms an integral part of the overall risk management framework.
- Where the draft RTS require policies, procedures, controls or tools already specified in detail under DORA, institutions may rely on those arrangements to fulfil the requirements.
- ICT-related incidents falling within the scope of operational risk are identified and treated as operational risk events, drawing on information already produced under DORA.
- The objective is a complete and consistent view of the institution's operational risk while avoiding duplication of requirements across the Union framework.



Question 1 Do respondents agree with the proposed approach in Article 2? Is any further clarification needed to avoid duplication?



Reporting, validation, audit and data governance

Reporting systems — Article 11

Regular, timely and robust reporting through the ordinary reporting lines. The management body in its supervisory function is informed at least quarterly (at least annually below EUR 750 million) on relevant data, the risk profile and appetite, material breaches, mitigation actions and lessons learnt; deficiencies are escalated ad hoc.

Audit — Articles 13 and 14

Risk-based review programme covering all significant activities, including third-party risk; data quality verified, including business indicator inputs; findings reported to the management body, which remains accountable where audit is outsourced.

Compliance routines and internal validation — Article 12

Compliance routines: top-level reviews of progress towards objectives, checks on approvals and authorisations, tracking of exceptions, overrides and deviations. Internal validation is a process, not a function: it periodically assesses the more quantitative and accounting elements of the framework — the assessment system, the calculation of the business indicator component and of the annual operational risk loss, decision-making models other than regulatory models (including AI applications), and the reconciliation of accounting data with the loss data set.

Data flows and governance — Article 15

Ownership, data quality controls, audit trails, documented definitions, traceability and accessibility.

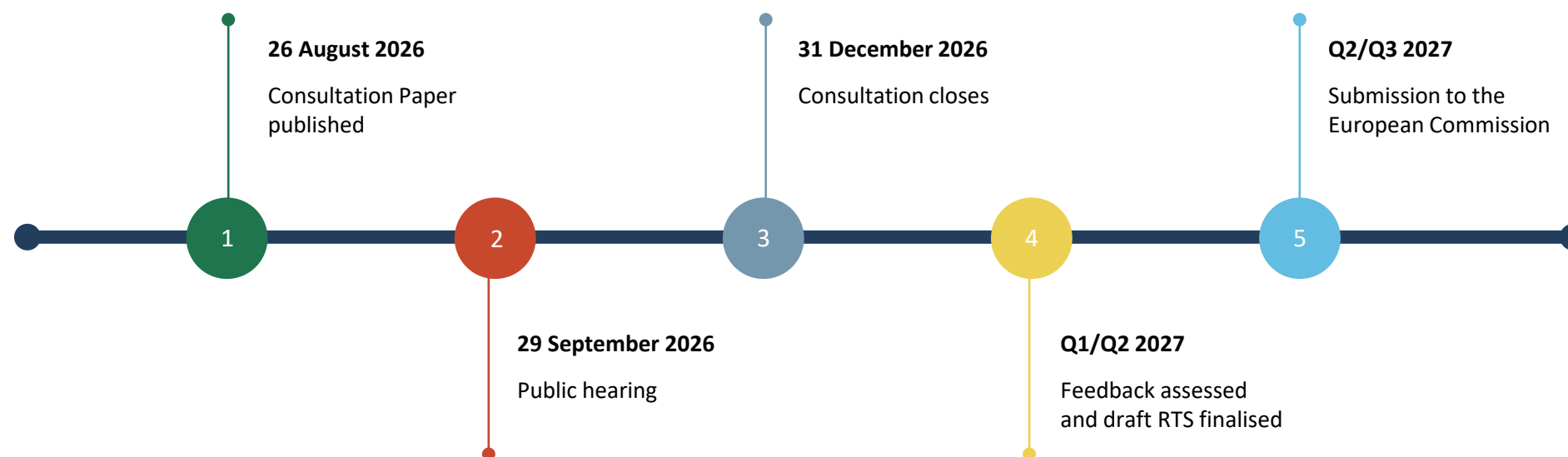


Questions 13–15 Are the proposed reporting requirements and frequencies appropriate, in particular below EUR 750 million (Q13)? Are the routines for ensuring compliance and the internal validation processes appropriate, including the requirements on models used for decision-making and the reconciliation of accounting data with the loss data set (Q14)? Do respondents agree with the requirements on transparent and accessible data flows and governance (Q15)?

Impact assessment — options considered and preferred options

	Options considered	Preferred option and rationale
Proportionality	(a) Relief based on the small and non-complex institution (SNCI) classification; (b) relief based on a business indicator below EUR 750 million	(b) — it covers more institutions, SNCI status is subject to supervisory discretion, and the business indicator is already the operational risk measure of size
Recording of losses	(a) No mapping of losses below EUR 20,000 and no recording obligation for small institutions; (b) mapping of relevant losses below that threshold	(b) — historical loss data is a cornerstone of operational risk management, and institutions may still tailor their own taxonomy
Costs	Establishment of systems and databases; hiring or internal reallocation of specialised staff	Mostly one-off, and close to zero for large institutions
Own funds	No change to the calculation of own funds requirements for operational risk	No costs associated with operational risk minimum capital requirements
Baseline rejected	Continuation of the status quo — heterogeneous application of generic rules without proportionate treatment	Maintains costs for small institutions and leaves large institutions without the data needed for a thorough assessment

Next steps and how to respond





Floor 24-27, Tour Europlaza
20 Avenue André Prothin
92400 Courbevoie, France

Tel: +33 1 86 52 70 00
E-mail: info@eba.europa.eu

<https://eba.europa.eu/>

QUESTIONS AND ANSWERS

Written responses through the EBA consultation page by 31 December 2026. This public hearing does not replace written responses.