EBA/CP/2026/18

26/08/2026

Consultation Paper

Draft Regulatory Technical Standards on operational risk management framework

Mandate under Art. 323(1) and (2) of Regulation (EU) 575/2013

Table of Contents

1. Responding to this consultation

The EBA invites comments on all proposals put forward in this paper and in particular on the specific questions summarised in 5.2.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices the EBA should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 31.12.2026. Please note that comments submitted after this deadline, or submitted via other means, may not be processed.

Publication of responses

Please clearly indicate in the consultation form if you wish your comments to be disclosed or to be treated as confidential. A confidential response may be requested from us in accordance with the EBA's rules on public access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the EBA's Board of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the EBA is based on Regulation (EU) 1725/2018 of the European Parliament and of the Council of 23 October 2018. Further information on data protection can be found under the Legal notice section of the EBA website.

2. Executive Summary

Article 323(1) of Regulation (EU) No 575/2013 (CRR), as amended by Regulation (EU) 2024/1623, requires institutions to have sound arrangements for the management of operational risk. Pursuant to Article 323(2) CRR, the EBA is mandated to develop draft regulatory technical standards (RTS) specifying those obligations, taking into consideration the size and complexity of the institution.

These draft RTS establish a harmonised minimum framework for the management of operational risk across institutions in the Union. They promote sound, effective and proportionate practices. They build on the revised prudential framework under the CRR and the Basel Committee's Principles for the Sound Management of Operational Risk.

The framework comprises three overarching components, for which the draft RTS define the key concepts. Governance sets out the responsibilities of t*he management body, including approval of the framework, definition of the operational risk appetite* and monitoring of the operational risk profile against it, and of senior management, which is empowered to implement the framework (though the responsibilities of its implementation lie ultimately with the management body) and translate that appetite into quantitative limits. Responsibilities span the three lines of defence, with the independent operational risk management function in the second line. The operational risk management process covers the ongoing identification, assessment, monitoring, control, mitigation and reporting of operational risk. The operational risk assessment system includes the calculation of the business indicator component and, for institutions with a business indicator equal to or exceeding EUR 750 million, of the annual operational risk loss, together with forward-looking tools.

The draft RTS further specify requirements on operational risk data and taxonomy, reporting systems, compliance routines, internal validation, audit and data governance, and allow reliance on DORA arrangements embedded within the overall risk management framework. Through this consultation, the EBA seeks stakeholders' views on the proposed framework.

Proportionality provisions

The draft RTS apply to all institutions, as all must have an operational risk management framework in place. The size and complexity of the business model are, however, considered in: (a) the frequency of the effectiveness review; (b) the expression of the operational risk appetite; (c) the extent of the data collected; (d) the alignment of the operational risk taxonomy; and (e) the reporting frequency to the management body. In addition, institutions with a business indicator below EUR 750 million are not required to collect the extended data set or report more often than annually.

Next steps

The EBA will consider the feedback received to this consultation in finalising the draft RTS. The final draft RTS will then be submitted to the European Commission for adoption in accordance with Article 10 of Regulation (EU) No 1093/2010.

3. Background and rationale

1. The EBA is consulting on draft Regulatory Technical Standards (RTS) requested by Article 323(2) of the Capital Requirements Regulation (EU) 575/2013 (CRR)[1] to specify the obligations under paragraph 1 of that Article, points (a) to (h), taking into consideration the size and complexity of the institution. This mandate aims to establish harmonised minimum requirements for institutions' operational risk management frameworks, ensuring robust, effective and proportionate practices across institutions of varying size, structure and business models.

3.1. Background

2. Regulation (EU) No 575/2013, as amended by Regulation (EU) 2024/1623[2], sets out in Article 323(1) a number of requirements that institutions have to implement for the management of operational risk. Those include a well-documented operational risk assessment and management system, an operational risk management function that is independent from the institution's business and operational units, regular reporting on operational risk exposures and losses, routines for ensuring compliance, internal validation processes, regular reviews by the audit function, and transparent and accessible data flows and processes associated with the operational risk assessment system.

3. The banking package implementing the final elements of Basel III in the European Union revises the prudential framework for operational risk own funds requirements. In particular, the previous approaches for calculating own funds requirements for operational risk, including advanced measurement approaches, are replaced by a single standardised approach. While this revised framework improves comparability and simplicity for Pillar 1 purposes, it also reinforces the importance of ensuring that all institutions maintain sound and effective arrangements for identifying, assessing, monitoring, controlling, mitigating and reporting operational risk, irrespective of whether they previously relied on simpler or more advanced prudential approaches.

4. Under the previous prudential framework, institutions using advanced measurement approaches were subject to more detailed supervisory expectations regarding governance, data, validation, scenario analysis and independent review. Although the revised framework no longer relies on internal models for the calculation of Pillar 1 own funds requirements for operational risk, supervisory experience gained under that framework remains relevant from a risk management and supervisory perspective. In particular, that experience has demonstrated the importance of strong governance, robust internal loss data collection, sound scenario-based assessments, effective challenge by independent internal control functions, and strong

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02013R0575-20260101
[2] https://eur-lex.europa.eu/eli/reg/2024/1623/oj

validation and audit arrangements. Those disciplines remain relevant for all institutions, albeit in a manner proportionate to their size, complexity, business model and operational risk profile.

5. The Basel Committee's Principles for the Sound Management of Operational Risk[3] provide an internationally recognised benchmark for operational risk governance and risk management. Those principles emphasise that operational risk management should be fully integrated into the institution's overall risk management framework, supported by effective governance, embedded in business processes, and informed by appropriate internal reporting and escalation. They also stress the importance of a sound risk culture, comprehensive risk identification and assessment, the use of relevant internal and external data, and independent review. These draft RTS are consistent with those internationally recognised supervisory principles and translate them into a harmonised minimum set of requirements under the CRR mandate.

6. Operational risk management is also closely connected to operational resilience. The Basel Committee's Principles for Operational Resilience[4] recognise that operational risk management and operational resilience are complementary and mutually reinforcing, since a sound operational risk management framework underpins an institution's ability to continue to deliver critical operations through disruption. At Union level, operational resilience forms an integral objective of the sound governance arrangements and effective internal control mechanisms required pursuant to Article 74 of Directive 2013/36/EU (CRD). By strengthening the identification, assessment, monitoring, control, mitigation and reporting of operational risk, these draft RTS support and reinforce institutions' operational resilience.

7. The draft RTS are also consistent with established Union supervisory frameworks, in particular the EBA Guidelines on internal governance. Operational risk cannot be managed in isolation from the institution's wider governance and internal control framework. Sound internal governance arrangements require a clear organisational structure, prudent and effective management, well-defined responsibilities across the three lines of defence, and robust reporting and escalation mechanisms. These elements are particularly relevant for operational risk, given that such risk may arise across all business lines, support functions, processes, systems and external dependencies. The draft RTS therefore clarify how the operational risk management framework is to be embedded within institutions' overall governance arrangements, while remaining aligned with existing governance requirements and avoiding unnecessary duplication.

8. The draft RTS also take into account the EBA Guidelines on the management of ESG risks (EBA/GL/2025/01) and the Guidelines on the sound management of third-party risk. Taking these Guidelines into account helps ensure that the draft RTS are consistent with the broader EBA regulatory framework and support a coherent, risk-based approach to prudential

[3] https://www.bis.org/bcbs/publ/d515.htm

[4] Basel Committee on Banking Supervision, Principles for Operational Resilience, March 2021, available at https://www.bis.org/bcbs/publ/d516.htm .

supervision. The draft RTS finally take into account Regulation (EU) 2022/2554 (DORA)[5], which establishes detailed requirements for ICT risk management, ICT-related incident handling and reporting, digital operational resilience testing, and ICT third-party risk management. ICT risk is a major driver of operational risk in the financial sector, and disruptions stemming from cyber incidents, ICT failures, data integrity problems or weaknesses in ICT third-party arrangements can have significant prudential implications. To ensure coherence within the Union framework and avoid duplication, the draft RTS require institutions to integrate ICT risk management into the broader risk management framework while allowing them to rely on policies, procedures, processes and controls already established under DORA to fulfil the requirements of these draft RTS.

3.2. Policy rationale

9. Operational risk may arise from inadequate or failed internal processes, people and systems or from external events, including legal risk events, misconduct events, failures in arrangements with third-party service providers and ICT-related incidents. It may affect institutions through multiple channels and may materialise across different business lines, support functions, legal entities and external dependencies. For that reason, an effective operational risk management framework should not be limited to the recording of realised losses. It should also support a sufficiently forward-looking understanding of operational risk exposures, including through the use of risk and control assessments, key indicators, scenario analysis, stress testing, near-miss information, business process mapping, and the monitoring of relevant internal and external developments. The framework should enable institutions to identify not only events and losses, but also vulnerabilities, control deficiencies, trends, patterns and emerging threats, so that corrective and preventive actions can be taken before risks crystallise.

10. At the same time, the EBA considers that proportionality is essential to ensure that the requirements of these draft RTS are effective and practicable across the wide range of institutions subject to the CRR. Institutions differ materially in terms of size, legal structure, product range, geographical footprint, degree of digitalisation, organisational complexity, reliance on third-party service providers, and overall operational risk profile. A uniform and highly prescriptive approach would risk imposing disproportionate burdens on smaller or less complex institutions without necessarily improving risk management outcomes. Accordingly, these draft RTS adopt a principle-based approach that specifies harmonised minimum obligations while allowing institutions to use simpler arrangements where justified by their size and complexity, provided that those arrangements remain effective. This proportionate approach is reflected, among other things, in the frequency of reviews and reporting, the degree of granularity of documentation and data collection, and the differentiated expectations for institutions with a business indicator below EUR 750 million and those with a business indicator equal to or exceeding that threshold.

[5] https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

11. The operational risk management framework specified in these draft RTS comprises three interrelated components. The first component is governance, including the responsibilities of the management body the senior management, and the internal control functions, including the operational risk management function. The second component is the operational risk management process, namely the policies, processes and procedures used to identify, assess, monitor, control, mitigate and report operational risk. The third component is the operational risk assessment system, including the methods, data, taxonomy, indicators and analyses that support the assessment of the institution's operational risk profile. These three components are mutually reinforcing and should operate as an integrated whole within the institution's broader governance, risk management and operational resilience arrangements.

12. With regard to governance, the RTS clarify that the management body in its supervisory function should approve the operational risk management framework and the institution's operational risk appetite, the management body in its management function should be responsible for implementing the framework and the senior management should ensure that operational risk exposures remain within the approved appetite and associated limits. In line with established supervisory expectations, institutions should maintain – as part of the internal controls - an operational risk management function that is independent from the business and operational units whose activities it oversees. That independence means that the function should not be responsible for the day-to-day management, operation or performance of the activities, processes or systems subject to its oversight, should be free from conflicts of interest, and should be able to provide objective challenge and advice without undue influence. The function should have sufficient authority, stature, resources and expertise and should report through appropriate channels to senior management and the management body. Clear accountability, appropriate reporting lines and timely escalation are necessary to ensure that operational risk is managed on an institution-wide basis.

13. With regard to the operational risk management process, the draft RTS set out minimum expectations for the ongoing identification, assessment, monitoring, control, mitigation and reporting of operational risk. This includes the need for institutions to embed operational risk management in day-to-day decision-making, product and process governance, change management, incident management, third-party arrangements decisions, remediation planning, internal communication and staff awareness. Operational risk management should not be treated as a stand-alone compliance exercise; rather, it should be integrated into ordinary management processes and should inform decisions concerning strategy, organisation, processes, systems, controls, third-party services and remediation measures.

14. With regard to the operational risk assessment system, the RTS specify minimum requirements for the collection and use of relevant operational risk information, including loss data, incidents, near misses, boundary cases, key indicators, scenario analysis, stress testing, risk and control assessments, and relevant internal and external factors. Robust data and taxonomy arrangements are necessary not only for compliance with prudential and reporting requirements, but also for effective internal risk analysis and management action. Institutions should be able to identify and classify operational risk events consistently, distinguish relevant

events from immaterial ones, analyse drivers and root causes, aggregate information across business lines and legal entities, and understand how operational risk exposures evolve over time. In this regard, the RTS set more granular expectations for institutions with a business indicator equal to or exceeding EUR 750 million and a simpler and more proportionate approach for institutions with a business indicator below that threshold. The table below summarises the main elements of this proportionality approach.

Area	Business indicator below EUR 750 million	Business indicator equal to or exceeding EUR 750 million
Review of the effectiveness of the framework	At least every two years	At least annually
Operational risk appetite	The business indicator, or its relevant components, may be used as the only proxy	Translated into quantitative limits, with exposures monitored against them
Operational risk data	Reduced set, including relevant and material loss data below EUR 20,000	Extended set, including relevant loss data below EUR 20,000, near misses, scenario analysis and stress testing results, and key risk and control indicators
Operational risk taxonomy	Recommended to be consistent with the RTS on operational risk taxonomy (for losses of any amount)	Required to be consistent with the RTS on operational risk taxonomy (for losses below EUR 20,000)
Reporting of the operational risk profile to the management body	At least annually	At least quarterly

15. With regard to the collection, maintenance and use of relevant data and information, the RTS request institutions to establish and maintain an operational risk taxonomy not only to classify the operational risk losses, but also for the classification of the operational risk events and the aggregation of the institution's operational risk profile across business processes and organisational levels. To support comparability and effective supervisory review, the RTS specify that institutions with a business indicator equal to or exceeding EUR 750 million should use a taxonomy consistent with the operational risk taxonomy established by Article 317(9) of the CRR, while those with a business indicator below that threshold are encouraged to do that.

16. The draft RTS require institutions to use the outputs of operational risk events, loss data, risk and control assessments, key indicators, scenario analyses and stress testing in a sufficiently forward-looking manner. Those tools are not intended to recreate internal models for the calculation of Pillar 1 own funds requirements. Rather, they are intended to support the setting and monitoring of operational risk appetite and limits, the identification of emerging risks (such as environmental, social and governance (ESG) risks, risks arising from the increasing use of artificial intelligence and other new technologies, and geopolitical risks), the prioritisation of remediation actions, the internal capital adequacy assessment process and the institution's

broader operational resilience approach. For smaller or less complex institutions, those tools may be implemented in a simpler manner, commensurate with the institution's risk profile.

17. The draft RTS also clarify expectations regarding reporting, compliance routines, internal validation and audit function. Regular reporting to senior management and the management body is essential to support informed decision-making and effective oversight. Institutions should also have mechanisms to identify, report and address non-compliance with internal policies, approved thresholds and limits, and applicable regulatory requirements. Internal validation and audit function serve distinct but complementary purposes: validation provides an independent assessment of the soundness and performance of key elements of the operational risk assessment system and related methodologies, while audit provides independent assurance on the adequacy and effectiveness of governance, controls, processes and data. In line with internationally recognised supervisory principles, including the Basel Committee's principles on independent review and validation, both functions should be organised in a manner that ensures sufficient independence, appropriate scope, timely reporting and effective follow-up of remedial actions.

18. Finally, the draft RTS address data flows and data governance in recognition of the fact that operational risk management increasingly depends on the availability, quality and traceability of data from multiple internal and external sources. Transparent and accessible data flows are essential for the reliability of operational risk assessment, reporting and supervisory review. Institutions should therefore establish clear ownership for operational risk data, document key data sources and data definitions, define minimum data quality controls, such as audit trails and, where relevant, loss data reconciliation procedures and ensure the accuracy, integrity completeness, timeliness, traceability and accessibility of the information used within the framework. More generally, the reliability of operational risk assessment and reporting depends on operational risk data being accurate, complete and produced in a timely manner, with data flow across the relevant systems, and on operational risk reporting to senior management and the management body being comprehensive, consistent and sufficiently granular to support sound operational risk management decisions. Institutions that fall within the scope of the Basel Committee's principles for effective risk data aggregation and risk reporting[6] should take those principles into account when developing their operational risk data and reporting arrangements.

19. Overall, these draft RTS aim to promote a common baseline for sound operational risk management across the Union, improve consistency in supervisory expectations, and strengthen institutions' capacity to identify and address operational risk in a forward-looking and proportionate manner. By clarifying the obligations in Article 323(1) of Regulation (EU) No 575/2013 and reflecting both internationally recognised principles and existing Union legislation, the draft RTS seek to enhance prudential soundness while preserving sufficient

[6] Basel Committee on Banking Supervision, Principles for effective risk data aggregation and risk reporting (BCBS 239), January 2013, available at https://www.bis.org/publ/bcbs239.htm .

flexibility for institutions to implement the requirements in a way that is commensurate with their risk characteristics.

4. Draft regulatory technical standards on institutions' arrangements for managing operational risk (Article 323, paragraph 1, points (a) to (h), and paragraph 2, of Regulation (EU) 575/2013)

Xxxx/xxxx

Commission Delegated Regulation (EU) 202x/xxxx

xxx

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms as amended by Regulation (EU) 2024/1623 and in particular to Article 323 thereof,

Whereas:

(1) Article 323, paragraph 1, of Regulation (EU) 575/2013 requires institutions to have in place a well-documented operational risk assessment and management system, an independent operational risk management function, regular reporting on operational risk exposures and losses, routines for ensuring compliance and internal validation processes, regular reviews by the audit function, and transparent and accessible data flows and processes associated with the operational risk assessment system. To ensure a harmonised application of those requirements across the Union, it is necessary to lay down detailed rules specifying further those arrangements.

(2) The prudential framework for operational risk under Regulation (EU) 575/2013 has been revised to improve comparability and simplicity in the calculation of own funds requirements. That revision does not lessen the need for institutions to maintain sound internal arrangements for the identification, assessment, monitoring, control, mitigation and reporting of operational risk. Sound operational risk management remains essential for the safety and soundness of institutions and for the stability of the financial system.

(3) Operational risk may arise from inadequate or failed internal processes, people and systems or from external events, including legal risk events, misconduct events, failures in third-party arrangements and ICT-related incidents. Given the breadth of its sources and transmission channels, operational risk should be managed through an institution-wide framework embedded in the overall governance and risk management arrangements of the institution.

(4) In specifying the requirements laid down in Article 323, paragraph 1, of Regulation (EU) 575/2013, account should be taken of internationally recognised supervisory standards, in particular the Basel Committee's Principles for the Sound Management of Operational Risk, as well as relevant Union supervisory guidance,

including the EBA Guidelines on internal governance, the EBA Guidelines on the management of ESG risks (EBA/GL/2025/01), the Guidelines on the sound management of third party risk and supervisory experience relating to advanced operational risk management practices. Those sources provide useful benchmarks for governance, independent review, data, reporting and the integration of operational risk management into business processes.

(5) Regulation (EU) 2022/2554 lays down uniform requirements concerning digital operational resilience for the financial sector. Since ICT-related risks, including ICT third-party risk, constitute a material component of operational risk for institutions, it is necessary to ensure consistency between the requirements laid down in this Regulation and those laid down in Regulation (EU) 2022/2554. Accordingly, ICT-related incidents that fall within the scope of operational risk should be identified and treated as operational risk events within the operational risk management framework, drawing where relevant on the information already produced under the ICT-related incident management and reporting arrangements established pursuant to that Regulation, so as to ensure a complete and consistent view of an institution's operational risk. To avoid duplication, institutions should be able to rely on strategies, policies, processes, ICT protocols and tools and controls established in accordance with Regulation (EU) 2022/2554, to the extent that those arrangements also satisfy the requirements laid down in this Regulation.

(6) The operational risk management framework should be proportionate to the size and complexity of the institution. Institutions differ materially in terms of organisational structure, nature and scope of activities, geographical footprint, use of technology, reliance on third-party services and overall operational risk profile. The requirements should therefore permit institutions to use simpler arrangements where justified by their size, provided that those arrangements remain effective.

(7) For the purpose of consistent application, it is appropriate to define certain terms that are key to the prudential management of operational risk, in particular the operational risk management framework, the operational risk profile and the operational risk appetite.

(8) Operational risk arises across the whole range of an institution's activities and is closely interconnected with the institution's other risks. For that reason, the operational risk management framework should be documented and should form an integral part of the institution's overall risk management framework. It should clearly allocate responsibilities between the management body in its supervisory and management function, senior management, business and internal control functions, and should support effective oversight, escalation and decision-making.

The framework should also be reviewed regularly to ensure that it remains appropriate in light of changes in the institution's activities, systems, organisation and external environment.

(9) Proper documentation is necessary to ensure the effectiveness, consistency and reviewability of the operational risk management framework. Institutions should therefore maintain up-to-date documentation covering the key elements of that framework, including governance arrangements, risk appetite, policies, procedures, controls, data arrangements and review mechanisms.

(10) The management of operational risk should be based on a continuous process of identifying, assessing, monitoring, controlling, mitigating and reporting operational risk. That process should be supported by appropriate policies, procedures and controls and should be communicated to the relevant staff and functions so that operational risk management is effectively embedded throughout the institution. Institutions should ensure that operational risks are identified, assessed and managed in context of the business activities and operational tasks in which the operational risk event may materialise. Sources of operational risk may originate from different internal or external functions, processes or organisational units, including functions provided or supported by a third party service provider, and potential effects on objectives may extend across multiple parts of the institution.

(11) An operational risk assessment system should provide a comprehensive and sufficiently forward-looking view of the institution's operational risk profile. To that end, institutions should use relevant information and analytical tools, which may include loss data, near-miss information, root cause analysis, risk and control assessments, business process mapping, key indicators, scenario analysis and stress testing, as appropriate to their size, complexity and operational risk profile. Moreover, since ESG factors may act as drivers of operational risk and may contribute to emerging operational risk exposures, the requirements laid down in this Regulation should be applied consistently with institutions' ESG risk management framework. More generally, operational risk is increasingly influenced by a range of emerging risk drivers, such as ESG factors, the growing use of artificial intelligence and other new technologies, and geopolitical developments, and institutions should adopt a sufficiently forward-looking approach in order to identify and assess such risks in a timely manner.

(12) Operational risk management should not be limited to ex-post loss recording or isolated control activities. To be effective, it should be integrated into the day-to-day operations of the institution, including product and process governance, change management, third-party services decisions, incident management, remediation

planning and internal communication arrangements. This would also reinforce the institution's approach to operational resilience.

(13) Reliable operational risk management requires the collection, maintenance and use of relevant data and information. Institutions should therefore establish and maintain a taxonomy not only to classify the operational risk losses, but also for the classification of the operational risk events and the aggregation of the institution's operational risk profile across business processes and organisational levels. For risk management purposes and for supporting comparability and effective supervisory review, institutions with a business indicator equal to or exceeding EUR 750 million should use a taxonomy consistent with the operational risk taxonomy established under Article 317(9) of the CRR for operational risk losses below EUR 20,000, while institutions with a business indicator below that threshold are encouraged to do that. In general institutions should collect operational risk data at a level of granularity appropriate to their size, complexity and risk profile. Institutions with more significant or complex operational risk exposures should be subject to more detailed expectations regarding the collection and classification of operational risk information.

(14) From an accounting perspective, all loss data should be recorded and included in the calculation of the business indicator. Additionally, institutions whose business indicator is equal to or exceeding EUR 750 million should identify and assess the relevance of operational risk losses below EUR 20,000 and record, store and manage those data where relevant. Institutions whose business indicator is below EUR 750 million should assess the relevance and materiality of operational risk losses below EUR 20,000 and record, store and manage those data accordingly. Although such losses are individually below the general recording threshold, they may, in aggregate, be indicative of recurring deficiencies or emerging operational risks, so that the selective capture of those that are relevant contributes to a more complete picture of an institution's operational risk profile. Institutions whose business indicator is equal to or exceeding EUR 750 million are, for that reason, expected to make the additional effort of identifying the losses that are relevant and of recording, storing and managing the corresponding data, whereas institutions whose business indicator is below EUR 750 million carry out, in addition, a materiality assessment, so that this effort remains proportionate to their size and to the nature, scale and complexity of their operational risk. Losses that are part of a pattern or highlight potential or known weaknesses in the institution's management of operational risk should be considered relevant operational risk losses. These losses should be classified according to a suitable taxonomy that allows the institution and the competent authority to analyse the data and detect potential deficiencies in the management of operational risk.

(15) An operational risk management function located within the second line of defence is necessary to ensure effective oversight and challenge of the implementation of the operational risk management framework. That function should be independent from the business and operational units whose activities it oversees, meaning that it should not be responsible for the day-to-day management, operation or control performance of the activities, processes or systems subject to its oversight. The function should be free from conflicts of interest, and should be able to provide objective challenge and advice without undue influence. It should have sufficient authority, stature, resources and expertise, and should report through appropriate channels to senior management and the management body. Its responsibilities should remain distinct from those of the audit function (third line of defence). The operational risk management function and the compliance function, when they do not coincide within the same organisational unit, should cooperate and exchange relevant information, particularly with regard to the management of legal risks. Their respective responsibilities, reporting lines and escalation procedures should be clearly documented.

(16) Reporting on operational risk exposures, losses, incidents, trends and remediation measures is necessary to enable senior management and the management body to discharge their oversight responsibilities. Institutions should therefore establish regular and ad hoc reporting arrangements that are commensurate with their operational risk profile and that ensure timely escalation of material issues.

(17) The soundness of an institution's operational risk management framework, and its continuing compliance with the relevant internal and external requirements, cannot be presumed once the framework has been established, since the institution's activities, processes and systems, and the operational risks to which they give rise, evolve over time. Institutions should maintain routines and procedures to ensure compliance with the operational risk management framework and with the relevant internal and external requirements. Internal validation processes should form part of those routines and should provide an independent assessment of the soundness and performance of the operational risk assessment system and related methodologies, where relevant.

(18) Regular review by the audit function is necessary to provide independent assurance regarding the adequacy and effectiveness of the operational risk management framework. The audit function should review the relevant policies, processes, controls and data on a risk-based basis and should report its findings in accordance with the institution's governance arrangements. Where internal audit activities are performed by a third-party service provider, responsibility for ensuring their proper performance should remain with the institution.

(19) The governance arrangements for internal validation and for audit relating to operational risk should ensure an appropriate scope of review, timely reporting of findings and effective follow-up of remedial actions. Validation and audit perform distinct but complementary roles and should be organised in a manner consistent with internationally recognised supervisory principles, including the Basel Committee's principles on independent review and validation. Those arrangements should reflect the institution's business developments and operational risk profile.

(20) Transparent and accessible data flows and processes are indispensable for the reliability of the operational risk assessment system. Institutions should therefore document key data sources, ownership and controls, such as audit trails and, where relevant, loss data reconciliation procedures, and should ensure that operational risk data are accurate, complete, timely, traceable, produced in a timely manner and sufficiently accessible for management and supervisory purposes.

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

(22) The European Banking Authority has 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 in accordance with Article 37 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council.

HAS ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Scope of application

1. This Regulation applies to institutions subject to Regulation (EU) 575/2013, on an individual and, where applicable, on a consolidated and sub-consolidated basis, in accordance with Part One, Title II of that Regulation.

Article 2

Integration with ICT risk management

1. Institutions shall ensure that ICT risk management, as required by Regulation (EU) 2022/2554 and directive (EU) 2022/2556, forms an integral part of their overall risk management framework.

2. Where this Regulation requires institutions to establish policies, procedures, controls or tools that are already specified in detail under Regulation (EU) 2022/2554, institutions may rely on these strategies, policies, procedures, controls or tools to fulfil the requirements of this Regulation.

Consultation box 1

Question 1: Do respondents agree with the proposed approach in Article 2? Please indicate whether any further clarification is needed to avoid duplication.

Article 3

Definitions

For the purposes of this Regulation, the following definitions shall apply:

1. 'operational risk management framework' means the overall framework for identifying, assessing, monitoring, controlling, mitigating and reporting operational risk, including the risk of non-compliance as defined in Article 4(1), point (52a), letters (e), (f) and (g), of Regulation (EU) No 575/2013. It comprises the governance arrangements for the management of operational risk, the operational risk management process, and the operational risk assessment system;
2. 'operational risk profile' means the representation, at a given point in time, of an institution's aggregated operational risk exposure, both current and forward-looking, taking into account the size, complexity, and risk characteristics of its activities;
3. 'operational risk appetite' means the aggregate level and types of operational risk exposure that an institution is willing to assume within its risk capacity, in line with its business model, in order to achieve its strategic objectives;
4. 'operational resilience' means the ability of an Institution to deliver critical or important functions through disruption;
5. 'business indicator' means the business indicator calculated in accordance with Article 314 of Regulation (EU) No 575/2013.

Consultation box 2

Question 2: Do respondents consider the proposed definitions of the operational risk management framework, operational risk profile and operational risk appetite to be sufficiently clear and aligned with Article 4(1), point (52a), and Article 323 of Regulation (EU) No 575/2013? Please identify any additional definitions that would be necessary.

CHAPTER II

OPERATIONAL RISK MANAGEMENT FRAMEWORK

Article 4

Establishment of the operational risk management framework

1. Institutions shall establish, implement and maintain a documented, institution-wide operational risk management framework that is fully integrated into the overall risk management framework across the institution and embedded in the institution's day-to-day operations. The operational risk management framework shall be supported by a clear organisational structure with well-defined, transparent and internally consistent lines of responsibility.
2. Institutions shall ensure that their operational risk management framework reinforces their operational resilience approach, making use of the mechanisms, resources and data employed for operational risk management in support of the delivery of critical or important functions through disruption.
3. The institution's management body shall:
    a. approve the operational risk management framework;
    b. define and approve, at least annually, the institution's operational risk appetite;
    c. monitor, on a continuous basis, that the operational risk profile is within the operational risk appetite.
4. Institutions with a business indicator equal to or exceeding EUR 750 million shall evaluate, at least annually, and institutions with a business indicator below EUR 750 million shall evaluate, at least every two years, the effectiveness of the operational risk management framework and shall take appropriate remedial actions where deficiencies are identified.
5. The management body in its management function shall be responsible for implementing the operational risk management framework approved by the

management body in its supervisory function and the Senior Management shall be empowered to implement the related policies, processes, procedures and systems necessary to manage operational risk.

6. Senior management shall manage the operational risk profile within the operational risk appetite by translating the operational risk appetite into quantitative limits, such as limits based on loss metrics. Senior management shall monitor operational risk exposures against those limits. Escalation procedures shall be established for breaches of those limits.

7. Institutions whose business indicator is below EUR 750 million may use the business indicator, or its relevant components, as the only proxy for the operational risk appetite of the institution or for the allocation of that appetite throughout the institution. The competent authority may require additional quantitative measures if the business model or the risk profile of the institution would be misrepresented by using only the business indicator or its relevant components.

Consultation box 3

Question 3: Do respondents agree with the proposed responsibilities of the management body in its supervisory and management function and senior management for the establishment, approval, implementation, management and monitoring of the operational risk management framework? In particular, do respondents agree with the proposed use of the business indicator, or its relevant components, as a proxy for operational risk appetite for institutions with a business indicator below EUR 750 million? What are your views on the use of past operational risk losses when setting or allocating their operational risk appetite? What other measures, indicators, or limits do respondents use to set their risk appetite?

Article 5

Documentation of the operational risk management framework

1. Institutions shall have policies in place setting out standards to ensure the high quality of internal documentation related to the operational risk management framework. Those policies shall assign specific responsibilities for ensuring that such documentation is complete, consistent, accurate, up to date, appropriately approved and securely retained.

2. The policies referred to in paragraph 1 shall define the minimum content of documentation, including at least author, version number, body responsible for approval and dates of development and approval.

3. The documentation of the operational risk management framework shall clearly:

a. identify the governance structures used to manage operational risk, including reporting lines and accountabilities, and the mandates and membership of the operational risk governance committees, where applicable;

b. reference the relevant operational risk management policies and procedures;

c. describe the roles and responsibilities with regard to operational risk across the three lines of defence, in line with the overall risk management framework;

d. describe the institution's operational risk appetite and the approved risk mitigation strategies;

e. describe the institution's operational risk treatment strategy, including the design, implementation and tested effectiveness of controls;

f. provide for appropriate independent review and challenge of the operation and outcomes of the risk management process; and

g. require the operational risk management framework to be reviewed and revised, as appropriate, on the basis of a continuous assessment of the control environment.

4. The documentation relating to the operational risk management framework shall be sufficiently detailed to permit an independent review by internal or external parties, including competent authorities.

Consultation box 4

Question 4: Do respondents agree with the proposed documentation requirements for the operational risk management framework? Are the minimum elements of documentation appropriate and proportionate to the size, complexity and operational risk profile of institutions?

Article 6

Operational risk management process

1. Institutions shall establish and maintain policies, processes and procedures for the management of operational risk as part of the operational risk management framework.

2. Institutions shall apply an ongoing operational risk management process to identify, monitor, control, mitigate and report operational risk and shall clearly identify the staff responsible for each component of that process.

3. Institutions shall ensure that the information resulting from the process referred to in paragraph 2 is communicated to those responsible within the institution for the management of operational risk, including the first line of defence, and to those responsible for managing activities that give rise to operational risk.
4. Institutions shall ensure the appropriate level of engagement in operational risk management and culture by the staff of the institution, including awareness of the operational risk exposure and of the policies, processes and procedures for the management of operational risk.
5. Institutions shall ensure that control activities are designed, implemented and applied in relation to operational risk sources, events and effects on objectives, including preventive measures addressing sources of risk, detective measures addressing the occurrence of events, and corrective measures addressing adverse effects on objectives, to an extent that ensures that operational risk exposures are kept within operational risk limits.

Consultation box 5

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? Please indicate whether further clarification is needed on Article 6(3), in particular as regards the scope, recipients and frequency of such communication.

Article 7

Operational risk assessment system

1. Institutions shall implement and maintain effective processes and procedures for the comprehensive identification and assessment of operational risk, which shall include the calculation of the business indicator component and, for institutions with a business indicator equal to or exceeding EUR 750 million, the calculation of the annual operational risk loss.
2. The operational risk assessment system shall enable:
    a. the identification and assessment, through a bottom-up as well a top-down approach of the operational risks in order to manage exposures within operational risk limits and, ultimately, within the operational risk appetite;
    b. the detection and accurate categorisation of the operational risk events, including cases where operational risk is intertwined with other risks, including with ESG risk which may constitute drivers of operational risk. Institutions shall be able to identify operational risks in a structured manner, including the sources of risk, the operational risk event and the resulting

impact on the institution's objectives, and subsequently analyse the drivers and root causes of such events; and

c. the use of all relevant information derived from operational risk events, including external events, for the forward-looking assessment of operational risk exposures and contributing to the internal capital adequacy assessment of the capital requirement.

3. Institutions shall apply appropriate assessment procedures, proportionate to their operational risk profile, including, where relevant:

   a. business process mapping, to identify key steps in business processes, activities and organisational functions, as well as the associated operational risks and areas of control weakness;

   b. risk and control assessments; and

   c. scenario analysis and stress testing.

4. Scenario analyses and stress testing of operational risk shall be conducted, with a level of sophistication, granularity and frequency proportionate to the institution's size, complexity and operational risk profile, for the following purposes:

   a. the internal capital adequacy assessment of the capital requirement for operational risk;

   b. informing decisions on establishing the operational risk appetite level and allocation of operational risk limits;

   c. assess operational risk exposures, threats and vulnerabilities under severe, but plausible, conditions, and integrate the results into the institution's operational resilience approach.

Consultation box 6

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?

Article 8

Integration of the operational risk management framework into day-to-day operations and decision-making

1. Institutions shall ensure that the operational risk management framework is embedded and used to manage operational risks across different business areas, units or legal entities within the organisational structure.
2. Institutions shall ensure the continuous integration of their operational risk management framework into their day-to-day operations and decision-making processes by ensuring that:
    a. the operational risk management framework is regularly updated and further developed as the institution gains experience and sophistication in the management and assessment of operational risk;
    b. the institution's definition of operational risk appetite and its associated operational risk management objectives and activities are clearly communicated within the institution;
    c. the relationship between the institution's business strategy and its operational risk management, including the approval of products, activities, systems and processes, is clearly communicated within the institution;
    d. a predetermined set of protocols is implemented within the institution for the identification, analysis, end-to-end management and reporting of operational risk events;
    e. the operational risk assessment system increases transparency, risk awareness and operational risk management expertise and creates incentives to improve the management of operational risk throughout the institution;
    f. the nature, quality and balance of inputs into the operational risk assessment system are relevant and reflect the institution's business model, strategy, organisation and operational risk profile at all times;
    g. the operational risk assessment system produces consistent and timely information that accurately reflects the nature of the business and the institution's overall operational risk profile, and that such information is available to relevant decision-makers; and
    h. the institution systematically uses the outputs of the operational risk assessment system for decision-making processes and plans, including, but not limited to, action plans, business and insurance plans, change management and the continuous improvement of the operational risk management framework.

Consultation box 7

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?

Article 9

Operational risk data, information and taxonomy

1. Institutions shall establish processes and procedures to:
    a. collect, record, store, aggregate, analyse and monitor operational risk data, ensuring that such data are accurate, complete, consistent and timely; and
    b. monitor internal and external factors that may provide indications of changes in operational risk exposures, including developments in the operating environment, threat landscape, business model and third-party arrangements.
2. For institutions with a business indicator equal to or exceeding EUR 750 million, the operational risk data and the internal and external factors referred to in paragraph 1 shall include, in addition to the operational risk loss data as indicated in Article 317, paragraph 1, of Regulation (EU) 575/2013, the following elements:
    a. where relevant, operational risk loss data below EUR 20,000. Institutions shall define, in their internal documents and procedures, the key criteria used to determine when operational risk loss data below EUR 20,000 is considered relevant for inclusion;
    b. incidents and near misses with no loss impact, and boundary cases, even where operational risk contributes to losses classified under other risk types;
    c. minimum information fields to support analysis of drivers and root causes of operational risk events, the consequences of operational risk and linkage to the relevant business processes;
    d. when appropriate, external operational risk loss data;
    e. results of scenario analysis and stress testing;
    f. outputs of risk and control assessments;
    g. key risk indicators and key control indicators;
    h. relevant financial and non-financial information, including contingent liabilities on operational risk; and

i. input and output data for the building of the business indicator and the calculation of the business indicator component, including the allocation of losses, expenses, provisions and financial impacts due to operational risk events to the appropriate profit and loss items.

3. For institutions with a business indicator below EUR 750 million, the operational risk data and the internal and external factors referred to in paragraph 1 shall include:

   a. where relevant, material operational risk loss data below EUR 20,000 and in any case above EUR 20,000, consistently with the criteria indicated in Article 317, paragraphs 3,5 and 6 and Article 318 of the CRR. Institutions shall define, in their internal documents and procedures, the key criteria used to determine when operational risk loss data below EUR 20,000 are considered relevant and material for inclusion; and

   b. the elements referred to in paragraph 2, points (b), (c), (d), (h) and (i).

4. Institutions shall ensure that operational risk data and internal and external factors are used to support the identification and assessment of operational risk, as well as monitoring, escalation, decision-making and remediation. Institutions shall take a forward-looking approach where relevant, especially when identifying and assessing ESG risks and emerging operational risks.

5. Institutions shall establish and maintain a procedure for the development and maintenance of an operational risk taxonomy that enables the consistent identification of operational risk events and the consistent classification, recording and analysis of materialised operational risk events. The taxonomy shall support the aggregation of the operational risk profile across relevant business processes and relevant organisational levels.

6. The taxonomy shall be tailored to the institution's size, nature, scale and complexity and shall be applied consistently across the institution. The procedure referred to in paragraph 5 shall define the minimum taxonomy elements and the way in which the taxonomy is governed, including ownership and change control.

7. For institutions with a business indicator equal to or exceeding EUR 750 million, the taxonomy used for the identification and classification of operational risk events for risk management and supervisory purposes shall be consistent with the applicable technical standards on operational risk loss data classification. Other institutions are recommended to base their taxonomy on those standards for risk management and supervisory purposes.

Consultation box 8

Question 8: Do respondents agree with the proposed requirements on operational risk data, information and taxonomy? In particular, do respondents agree with the use of the expression "where relevant" for operational risk loss data below EUR 20,000 for institutions with a business indicator equal to or exceeding EUR 750 million, and with the requirement for institutions to define the criteria for relevance in their internal documents and procedures? Should the concept of "relevance" be further developed?

Question 9: For institutions with a business indicator below EUR 750 million, do respondents consider the proposed threshold for collecting and classifying operational risk loss data to be proportionate? In particular, should the draft RTS retain the proposed approach based on losses above EUR 20,000 and relevant and material losses below that threshold, or should a different threshold be considered? What thresholds do respondents use internally for the recording of operational risk losses? Should the concepts of "relevance and materiality" be further developed? Please provide reasons and, where possible, supporting evidence.

Question 10: Do respondents agree that institutions with a business indicator equal to or exceeding EUR 750 million should ensure consistency between their taxonomy for supervisory purposes and the operational risk taxonomy developed under Article 317(9) of Regulation (EU) No 575/2013, while institutions with a business indicator below EUR 750 million are only recommended to base their taxonomy on those standards?

Question 11: The boundary cases referred to in Article 9.2 (b), whose losses are classified under other risk types, are considered those for which the institution calculates already a Pillar 1 regulatory capital. Besides market risk (whose losses are already included within the scope of operational risk by Art 317(6) of the CRR), these refer to credit risk, counterparty risk and CVA risk. Boundary cases with Pillar 2 risks, such as strategic risk, business risk, liquidity risk, should be always treated as operational risk so that those losses contribute to the operational risk regulatory capital (i.e. included into the business indicator) and, for institutions with a BI > EUR 750 mln, to the annual operational risk loss. Do respondents agree with this interpretation of boundary cases of operational risk and other risks treated under Pillar 1 or Pillar 2?

CHAPTER III

GOVERNANCE

Article 10

Independent operational risk management function

1. The operational risk management function, as part of the institution's second line of defence, shall, at a minimum, perform the following tasks independently of the institution's business and operational units:

    a. design, develop, maintain and oversee the operational risk management process and the operational risk assessment system;

    b. review and contribute to the monitoring and reporting of the operational risk profile;

    c. challenge the operational risk associated with the introduction or development of products, markets, lines of business, processes and systems, and with significant changes to existing products or activities, ensuring that the operational risk management process and operational risk assessment system remain aligned with the institution's operational risk profile

    d. oversee business activities that may give rise to operational risk exposures that could breach the institution's risk appetite, and recommend or monitor remedial actions where appropriate; and

    e. promote an operational risk management culture throughout the organisation, including by means of training and by setting targets for operational risk loss prevention and reduction.

2. The operational risk management function shall receive appropriate support and oversight from the management body and senior management and shall have adequate resources, authority and stature within the organisation to fulfil its tasks. Where certain types of operational risk are subject to oversight by other functions within the institution, the operational risk management function shall ensure, and be able to, evidence, that it maintains an independent, comprehensive and institution-wide view of such operational risks.

3. The operational risk management function shall not be responsible for the audit function, taking into account the audit function's role in challenging the operational risk management framework.

4. The head of the operational risk management function shall:

a. have an appropriate level of knowledge, expertise and experience to oversee the institution's actual and prospective operational risk, as indicated by the operational risk profile;

b. maintain regular and direct communication with the management body and its committees, in accordance with the institution's risk management framework;

c. actively participate in the development of the institution's operational risk appetite and the strategy for its management and mitigation; and

d. be independent of the operational units and functions overseen by the operational risk management function.

Consultation box 9

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 from business and operational units sufficiently clear and proportionate? If not, please specify which additional clarifications would be useful.
In particular, how would institutions position the operational risk management function in practice within the second line of defence, including in relation to other control functions such as risk management or compliance functions?

CHAPTER IV

REPORTING, VALIDATION AND AUDIT

Article 11

Reporting systems

1. Institutions shall have in place a system for reporting their operational risk profile that is sufficiently regular, timely and robust, ensuring at least the following:

a. operational risk reports follow the ordinary reporting lines of the institution's organisation, so that they are distributed to the appropriate levels of line management, risk committees and the areas of the institution identified in the reports as areas of concern;

b. Management body in its management function receives operational risk information, including the operational risk profile, and reports that

information to the management body in its supervisory function at least quarterly, or at least annually for institutions with a business indicator below EUR 750 million;

c. operational risk reports contain relevant management information on the operational risk profile of the institution and include at least a high-level summary of the top operational risks of the institution, its relevant subsidiaries and its business units. As a minimum, the reports shall include information on:

   i. relevant operational risk data and internal and external factors, as referred to in Article 9;

   ii. the institution's operational risk profile and appetite;

   iii. material breaches of the operational risk appetite; and

   iv. mitigation actions, as well as lessons learnt;

d. ad hoc reports are produced and escalated in a timely manner to the appropriate level of management when deficiencies are identified in the policies, processes and procedures for managing operational risk, in order to ensure their prompt detection and remediation; and

e. problems relating to the institution's reporting systems and internal controls are identified promptly and accurately.

Consultation box 10

Question 13: Do respondents agree with the proposed operational risk reporting requirements, including the regularity of reports, the use of ordinary reporting lines and the escalation of deficiencies? Are the proposed reporting frequencies appropriate, in particular for institutions with a business indicator below EUR 750 million?

Article 12

Routines for ensuring compliance and Internal validation processes

1. Institutions shall have in place routines and procedures to ensure continuous compliance with the operational risk management framework, including, where relevant:

a. top-level reviews of progress towards stated objectives;

b. evaluation of the required approvals and authorisations to ensure accountability at an appropriate level of management; and

c. tracking of reports on approved exceptions to thresholds or limits, management overrides, and other deviations from internal policies, regulatory requirements and applicable laws.

2. The routines and procedures referred to in paragraph 1 shall include internal validation processes that periodically assess, at least:

a. the operational risk assessment system and the processes for the calculation of the business indicator component and, for institutions with a business indicator equal to or exceeding EUR 750 million, the process for the calculation of the annual operational risk loss; and

b. where models are used for decision-making purposes, such as for product pricing, artificial intelligence applications, the evaluation of financial instruments or client profiling, the soundness of the models used to identify and mitigate model risk, other than regulatory models;

c. the reconciliation between the accounting data relating to operational risk losses and the operational risk loss data set.

3. The outcomes of the internal validation processes shall be documented and shall be suitable both for the institution's internal decision-making and for supervisory review.

4. Institutions shall adopt and maintain policies and procedures to identify, report and address, in a timely manner, any instance of non-compliance.

Consultation box 11

Question 14: Do respondents agree with the proposed routines for ensuring compliance and the internal validation processes? Are the requirements on models used for decision-making purposes sufficiently clear, including their interaction with model risk management requirements outside regulatory models? Should the reconciliation between accounting data relating to operational risk losses and the operational risk loss data set be included within the internal validation processes?

Article 13

Audit reviews

1. Institutions shall ensure that their audit function assesses and confirms that the operational risk management process and the operational risk assessment system are reliable and effective in managing and assessing operational risk within the institution.

2. Institutions shall ensure that the audit function verifies, at a frequency commensurate with the institution's operational risk profile, the integrity of the operational risk policies and the most relevant processes and procedures, including their compliance with regulatory requirements and established internal controls. In particular, the audit function shall assess the quality, accuracy and completeness of the sources and data used for operational risk management and assessment purposes, including for the calculation of the business indicator component.

3. Institutions shall ensure that the audit function maintains a review programme covering the operational risk management framework, which is regularly updated to reflect:

    a. developments in internal processes for identifying, assessing, monitoring, controlling, mitigating and reporting operational risk; and

    b. the implementation of new or material changes to existing products, processes and systems that may expose the institution to material operational risk.

4. Where audit activities are carried out by internal or external audit functions, institutions shall ensure that those functions are independent of the activities, processes or systems under review and appropriately qualified to conduct the reviews. Where audit activities are performed by a third-party service provider, the management body shall remain accountable for ensuring that those activities are performed in accordance with the institution's approved audit plan.

5. Institutions shall ensure that audit reviews relating to the operational risk management framework are properly documented and that their outputs are distributed to the appropriate recipients within the institution.

6. Institutions shall ensure that the findings of the internal or external audit functions are promptly taken into account considering their severity and effectively implemented in the management of operational risk.

Article 14

Audit and internal validation governance

1. Institutions shall ensure that the results of audit reviews of the operational risk management framework and internal validation processes are summarised and reported in a timely manner to the management body or to a committee designated by it for approval.

2. Institutions shall ensure that the governance of audit and internal validation activities related to operational risk is of high quality. In particular, institutions shall ensure that:

    a. audit programmes cover all significant activities that could expose the institution to material operational risk, including third-party risk; and

    b. internal validation processes are proportionate to changes in the institution's business, operating environment and operational risk profile, and that their outcomes are subject to audit review.

Article 15

Operational risk data flows and governance

1. As part of their risk data aggregation and reporting framework, institutions shall establish and maintain procedures that ensure accurate, complete, timely, transparent and traceable operational risk data flows and processes associated with the operational risk assessment system. Those procedures shall cover, where relevant, the end-to-end flow from capture to classification, aggregation, analysis, reporting and retention of operational risk data and relevant internal and external factors.

2. Institutions shall ensure clear data flow across all relevant systems. Risk reports submitted to senior management shall be comprehensive, clear and appropriately detailed, having regard to the size and complexity of the institution and the nature of its operational risk profile, so as to support sound operational risk management decisions.

3. Institutions shall assign ownership for operational risk data and internal and external factors, and shall define minimum data quality controls, such as audit trails and, where relevant, reconciliation procedures between the accounting data relating to operational risk losses and the operational risk loss data set, ensuring accuracy, integrity, completeness, timeliness, traceability and accessibility of the information used within the operational risk framework.

4. Institutions shall ensure that operational risk reporting is supported by documented data definitions and that users of operational risk information can understand the origin, meaning and limitations of the underlying data.

Consultation box 12

Question 15: Do respondents agree with the proposed requirements on transparent and accessible operational risk data flows and governance, including ownership, data quality controls, data definitions, traceability and audit trails?

Consultation box 13

Question 16: Do respondents consider the differentiation based on the business indicator threshold of EUR 750 million to be appropriate, or should different but equally simple and consistent metrics be introduced? More generally, is proportionality sufficiently reflected throughout the draft RTS, including in relation to data collection and loss thresholds for institutions with a business indicator below EUR 750 million? If not, please provide examples and suggestions.

5. Accompanying documents

5.1. Draft cost-benefit analysis / impact assessment

Article 323(1) of Regulation (EU) No 575/2013 (CRR), as amended by Regulation (EU) 2024/1623, requires institutions to have in place sound arrangements for operational risk management, including a well-documented operational risk assessment and management system integrated into day-to-day risk management processes, an independent operational risk management function, a system of reporting to senior management, procedures for taking appropriate corrective actions, routines for ensuring compliance, internal validation processes, regular audit reviews, and transparent and accessible data flows and processes associated with the operational risk assessment system.

Pursuant to Article 323(2) of the CRR, the EBA is mandated to develop draft regulatory technical standards (RTS) specifying those obligations, taking into consideration the size and complexity of the institution.

5.1.1. Problem identification

The current landscape of the operational risk management appears rather heterogeneous amongst the various credit institutions that apply the relevant processes, let alone that some of these institutions may apply monitoring practices or risk management procedures that do not comply with their size, complexity and systemic importance of these institutions. For example, there might be systemically important institutions that apply rather simplistic processes, or lack dedicated staff, for the assessment and management of operational risk.

These draft RTS streamline the application of the operational risk management processes by providing a harmonised minimum framework for the management of operational risk across institutions in the Union, considering the need for proportionate treatment of institutions that do not pose an unduly high systemic risk to the EU banking system via their operational risk exposures.

In doing so, the draft RTS build on the revised prudential framework for operational risk under the CRR, the Basel Committee's Principles for the Sound Management of Operational Risk, the EBA Guidelines on internal governance, and the Union framework on digital operational resilience established by Regulation (EU) 2022/2554 (DORA).

In addition, the harmonisation of the rules, at Level 2 Regulation, addresses potential information asymmetries, arising from the lack of dedicated operational risk functions, and behavioural biased, e.g. disproportional application due to misinterpretation of the Level 1 operational risk framework.

The abovementioned factors justify the regulatory intervention at Level 2 Regulation and, subsequently, the conduct of an impact assessment to identify the operational objectives aiming to resolve the identified problems.

Finally, the draft RTS considered the outcome of a high-level qualitative impact assessment that was deemed most appropriate for the nature of the identified problem and provided by the framework set by the EBA mandate as depicted in the CRR.

5.1.2. Policy objectives

The various provision of the draft RTS is the outcome of a thorough qualitative impact assessment, that took place during the deliberations amongst the Member States, and addresses the following strategic (generic) objective, set out by the Article 323(2) of the CRR, and the operational (specific) objectives set out by the EBA during the deliberations.

Strategic objective: an Operational risk management framework as set out by Article 323(1) of the CRR; and,

Operational objectives: identify the technical provisions that would enable proportionality of the application of the strategic objective and effective monitoring and management of operational risk functions, without hampering the harmonised application of the rules.

5.1.3. Baseline scenario

The baseline scenario, aka “do nothing scenario”, for this draft RTS would be the continuation of the status quo, i.e. universal application of the generic operational risk framework that implies heterogeneous application of generic rules, without proportionate treatment of a subset of credit institutions that don’t need in-depth assessment of the operational risk exposures. This treatment would result to increased costs, or to maintenance of increased costs, for small institutions and no thorough assessment of the operational risk exposures for large institutions which need additional data to conduct such assessments.

5.1.4. Options considered

Following the rejection of the baseline scenario, the EBA examined several options to address the effective application of proportionality in the operational risk management and the collection of additional data for the effective monitoring and management of operational risk exposures

Proportionality: the Level 1 text of the EU Regulation (Art. 323(2) of the CRR3) requires the EBA to consider proportionality when developing the RTS.

The EBA considered the following options:

(a) reduce the burden based on small and non-complex institutions (SNCI) classification, and

(b) reduce the burden based on a business indicator below EUR 750 million.

Recording of operational risk losses (Art. 9 of the RTS)

The Level 1 text mandates institutions with a business indicator equal or higher than EUR 750 million to have in place a loss data set and map losses above EUR 20,000 according to the taxonomy developed by the EBA.

The EBA considered the following options:

(a) Do not mandate institutions to map losses below EUR 20,000 and do not mandate small institutions to record any losses,

(b) Mandate institutions to map relevant losses below EUR 20,000 and mandate small institutions to map all losses above EUR 20,000 and material and relevant losses below EUR 20,000.

5.1.5. Cost-Benefit Analysis

The options on proportionality consider the level of application of the proposed rules. The costs associated with "proportionality" options are assessed vis-a-vis the baseline scenario, i.e. the "do nothing scenario". Both options are associated with negligible increased overall operational cost for the entire banking system, i.e. costs arising from the day-to-day functioning of credit institutions, that span from no increase for the large institutions to low increase for the smaller institutions. When comparing the two considered options on proportionality, i.e. "proportionality option (a)" vs. "proportionality option (b)" the EBA concluded that the costs associated with option (b) are marginally higher than option (a) due to the expanded coverage of institutions. Nonetheless, the negligibly elevated costs are counterbalanced by the enhanced monitoring capability that option (b) entails.

Regarding the options on the collection of operational risk data below EUR 20,000, the two options suggest only marginal additional costs as most of the institutions already collect this set of data, although they only use the subset of those above EUR 20,000 for the estimation of the annual operational risk loss. When comparing option (a) and option (b), the later entails a slightly higher operational cost, which is, similarly to the proportionality options, counterbalanced by the increased benefits of the enhanced monitoring and operational risk management capabilities.

Most of the costs described above are one-off and arise from the establishment of systems and databases, as well as with the hiring, or internal reallocation, of specialised personnel from small institutions. The costs for large institutions are close to zero.

There are no costs associated with operational risk minimum capital requirements arising from the abovementioned options.

5.1.6. Preferred option

The EBA option for “proportionality option (b)” because:

i. it encompasses more institutions (on average, SNCI have a business indicator well below EUR 750 million) that implies enhanced monitoring and management capacity of the EU banking system;
ii. some very small institutions are not SNCI because local supervisors used the supervisory discretion to keep them out of that label, so there was the risk that some very small institutions would have to apply the same rules of G-SIB; and,
iii. the concept of SNCI is not tied to operational risk, which actually uses the business indicator as an indicator of riskiness (not only for the EUR 750 million threshold, but also for the multiplier or Art. 313 CRR3).

The EBA opted for “loss data collection option (b)” because:

i. the historical loss data are a cornerstone of operational risk management for all institutions;
ii. the potential benefits of a robust operational risk management overbalance the cost of having in place a system to record and store the historical loss data; and,
iii. by not forcing institutions to use the EBA taxonomy, they can tailor their dataset to their needs, further reducing costs.

The RTS requires institutions with a business indicator equal or above EUR 750 million to record also losses below EUR 20,000 when they are relevant. To comply with the Level 1, the EBA encourages, but does not render it obligatory, these institutions to use the RTS developed by the EBA on the operational risk taxonomy for these losses; when these institutions choose not to use the operational risk taxonomy developed by the EBA for recording losses below EUR 20,000, they should adopt a taxonomy consistent with the one developed by the EBA. Similarly, the EBA also mandates institutions with a business indicator below EUR 750 million to record losses above EUR 20,000 (the use of the RTS developed by the EBA on the operational risk taxonomy is a recommendation, not obligation) and material losses below EUR 20,000.

5.2. Overview of questions for consultation

Question 1: Do respondents agree with the proposed approach in Article 2? Please indicate whether any further clarification is needed to avoid duplication.

Question 2: Do respondents consider the proposed definitions of the operational risk management framework, operational risk profile and operational risk appetite to be sufficiently clear and aligned with Article 4(1), point (52a), and Article 323 of Regulation (EU) No 575/2013? Please identify any additional definitions that would be necessary.

Question 3: Do respondents agree with the proposed responsibilities of the management body in its supervisory and management function and senior management for the establishment, approval, implementation, management and monitoring of the operational risk management framework? In particular, do respondents agree with the proposed use of the business indicator, or its relevant components, as a proxy for operational risk appetite for institutions with a business indicator below EUR 750 million? What are your views on the use of past operational risk losses when setting or allocating their operational risk appetite? What other measures, indicators, or limits do respondents use to set their risk appetite?

Question 4: Do respondents agree with the proposed documentation requirements for the operational risk management framework? Are the minimum elements of documentation appropriate and proportionate to the size, complexity and operational risk profile of institutions?

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? Please indicate whether further clarification is needed on Article 6(3), in particular as regards the scope, recipients and frequency of such communication.

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?

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?

Question 8: Do respondents agree with the proposed requirements on operational risk data, information and taxonomy? In particular, do respondents agree with the use of the expression “where relevant” for operational risk loss data below EUR 20,000 for institutions with a business indicator equal to or exceeding EUR 750 million, and with the requirement for institutions to define the criteria for relevance in their internal documents and procedures? Should the concept of “relevance” be further developed?

Question 9: For institutions with a business indicator below EUR 750 million, do respondents consider the proposed threshold for collecting and classifying operational risk loss data to be proportionate? In particular, should the draft RTS retain the proposed approach based on losses above EUR 20,000 and relevant and material losses below that threshold, or should a different threshold be considered? What thresholds do respondents use internally for the recording of operational risk losses? Should the concepts of "relevance and materiality" be further developed? Please provide reasons and, where possible, supporting evidence.

Question 10: Do respondents agree that institutions with a business indicator equal to or exceeding EUR 750 million should ensure consistency between their taxonomy for supervisory purposes and the operational risk taxonomy developed under Article 317(9) of Regulation (EU) No 575/2013, while institutions with a business indicator below EUR 750 million are only recommended to base their taxonomy on those standards?

Question 11: The boundary cases referred to in Article 9.2 (b), whose losses are classified under other risk types, are considered those for which the institution calculates already a Pillar 1 regulatory capital. Besides market risk (whose losses are already included within the scope of operational risk by Art 317(6) of the CRR), these refer to credit risk, counterparty risk and CVA risk. Boundary cases with Pillar 2 risks, such as strategic risk, business risk, liquidity risk, should be always treated as operational risk so that those losses contribute to the operational risk regulatory capital (i.e. included into the business indicator) and, for institutions with a BI > EUR 750 mln, to the annual operational risk loss. Do respondents agree with this interpretation of boundary cases of operational risk and other risks treated under Pillar 1 or Pillar 2?

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 from business and operational units sufficiently clear and proportionate? If not, please specify which additional clarifications would be useful. In particular, how would institutions position the operational risk management function in practice within the second line of defence, including in relation to other control functions such as risk management or compliance functions?

Question 13: Do respondents agree with the proposed operational risk reporting requirements, including the regularity of reports, the use of ordinary reporting lines and the escalation of deficiencies? Are the proposed reporting frequencies appropriate, in particular for institutions with a business indicator below EUR 750 million?

Question 14: Do respondents agree with the proposed routines for ensuring compliance and the internal validation processes? Are the requirements on models used for decision-making purposes sufficiently clear, including their interaction with model risk management requirements outside regulatory models? Should the reconciliation between accounting data relating to operational risk losses and the operational risk loss data set be included within the internal validation processes?

Question 15: Do respondents agree with the proposed requirements on transparent and accessible operational risk data flows and governance, including ownership, data quality controls, data definitions, traceability and audit trails?

Question 16: Do respondents consider the differentiation based on the business indicator threshold of EUR 750 million to be appropriate, or should different but equally simple and consistent metrics be introduced? More generally, is proportionality sufficiently reflected throughout the draft RTS, including in relation to data collection and loss thresholds for institutions with a business indicator below EUR 750 million? If not, please provide examples and suggestions.