EBA/CP/2014/08

12 June 2014

# Consultation Paper

## Draft Regulatory Technical Standards on assessment methodologies for the Advanced Measurement Approaches for operational risk under Article 312 of Regulation (EU) No 575/2013

# 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 12.09.2014. Please note that comments submitted after this deadline, or submitted via other means, may not be processed.

### Publication of responses

Please clearly indicate on the consultation form whether 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 (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 as implemented by the EBA in its implementing rules adopted by its Management Board. Further information on data protection can be found in the Legal notice section at the bottom of the EBA website.

# 2. Executive summary

Regulation (EU) No 575/2013 sets out requirements relating to the assessment under which the competent authorities permit institutions to use Advanced Measurement Approaches ('AMA') for own funds calculation and requirements for operational risk and, in Article 312(4)(a), mandates the EBA to prepare draft regulatory technical standards (RTS) in this area. The EBA must submit the draft RTS to the Commission by 31 December 2014.

These draft RTS are targeted to competent authorities in relation to institutions that want to use or are already using AMA for regulatory purposes. Competent authorities will only grant permission to use AMA where institutions prove that all the relevant qualitative and quantitative requirements set out in these RTS have been met. Competent authorities will also assess whether institutions meet these requirements on an ongoing basis following the granting of permission.

Under AMA, an institution uses its own internal model to calculate capital requirements respect to its operational risk profile. The elements that determine the operational risk profile of an institution comprise of operational risk data gathered internally, actual and constructed, and operational risk data taken from external sources.

With a view to ensuring uniform application across the European Union of the definition of operational risk established by Regulation (EU) No 575/2013 and avoiding inconsistencies in the determination of institutions' operational risk profile, these RTS clarify the scope of operational risk and the scope of operational risk loss and specify common standards for the supervisory assessment of the governance of operational risk, in particular with respect to the role and responsibilities of the operational risk management function and the reporting system. These RTS also set out standards for the supervisory assessment of key components of the operational risk measurement system, ensuring that it is based on a well-founded methodology, that it is effective in capturing the institutions' actual and potential operational risk, that it is reliable and robust in generating AMA regulatory capital requirements and that it is comparable across institutions. These RTS also establish criteria for supervisory assessment of an institution's data quality and IT systems, 'use test' requirement and terms and the scope of audit and internal validation of the AMA framework.

These RTS will replace all the following CEBS guidelines that address AMA institutions: the 'Guidelines on the Implementation, Validation and Assessment of Advanced Measurement (AMA) and Internal Ratings Based (IRB) Approaches' (GL-10 CEBS, issued in 2006), limited to Section 4.3 and Annexes IV and V, the 'Compendium of Supplementary Guidelines on implementation issues of operational risk' (GL-21 CEBS, issued in September 2009), limited to the individual guidance papers 'Guidelines on the use test for AMA institutions' and 'Guidelines on the allocation of the AMA capital', and the 'Guidelines on Operational Risk Mitigation Techniques' (GL-25 CEBS, issued on 22 December 2009). These RTS also rely on:

- the 'Guidelines on the scope of operational risk and operational risk loss', included in the above mentioned CEBS 'Compendium of Guidelines', which will be replaced by these RTS for the parts referring to the AMA institutions only([1]);

- the Basel Committee 'Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches' (issued in June 2011) and 'Recognizing the risk-mitigating impact of insurance in operational risk modelling' (issued in October 2010);

- the standards published by industry consortia for the collection and reporting of operational risk data; and

- the experience gained by the supervisors since these Guidelines were issued.

The EBA believes that all EU Member States should assess the permission to use the AMA for operational risk in the same way in view of the establishment of the single rule book, and believes these RTS will encourage this objective.

Following the consultation, the EBA will review the RTS proposals to ensure that they take into account any changes arising from the consultation process.

[1] The 'Guidelines on the scope of operational risk and operational risk loss' will therefore continue to be valid with regard to the parts that do not strictly refer to AMA institutions.

# 3. Background and rationale

For purposes of own funds requirements for operational risk, Article 312(2) of Regulation (EU) No 575/2013 allows competent authorities to permit institutions to use AMA based on institutions' operational risk measurement systems, provided that all qualitative and quantitative standards set out in Articles 321 and 322 of Regulation (EU) No 575/2013 are met and provided that institutions meet the general risk management standards set out in Articles 74 and 85 of Directive 2013/36/EU([2]).

According to Article 312(4) the EBA is required to develop draft technical standards, to be submitted by the EBA to the Commission, to specify the following:

> (a) The assessment methodology under which the competent authorities permit institutions to use Advanced Measurement Approaches;
>
> (b) The conditions for assessing the materiality of extensions and changes to the Advanced Measurement Approaches;
>
> (c) The modalities of the notification required in paragraph 3 of Article 312 of the CRR.

The EBA has developed this Consultation Paper on the draft RTS on assessment methodologies for the AMA in accordance with the mandate contained in Article 312(4)(a) of Regulation (EU) No 575/2013. Points (b) and (c) of this Article have been included in the RTS on the 'Conditions for assessing the materiality of extensions and changes of internal approaches when calculating own funds requirements for credit and operational risk', which were adopted by the Commission on 12 March 2014, on the basis of the draft RTS prepared by the EBA([3]). These draft RTS should therefore be read in conjunction with the RTS on the 'Conditions for assessing the materiality of extensions and changes of internal approaches when calculating own funds requirements for credit and operational risk'.

Similar mandates exist for credit and market risk models, which are currently under development. In order to ensure a similar approach across all internal models in the capital requirements framework, some amendments to the wording of these RTS may be introduced at a later stage to ensure consistency.

These RTS should enable harmonisation across all EU Member States on how to assess the permission for institutions to use, and to continue to use, the AMA for operational risk.

[2] OJ L 176 of 27.6.2013, p. 338.

[3] http://www.eba.europa.eu/regulation-and-policy/model-validation/draft-regulatory-technical-standards-on-the-conditions-for-assessing-the-materiality-of-extensions-and-changes

## Main points of the draft RTS

Under an AMA, an institution uses its own internal model to calculate capital requirements with respect to its operational risk profile. The elements used to determine the operational risk profile of an institution comprise operational risk data gathered internally, actual and constructed, and operational risk data taken from external sources. This profile, in turn, depends on the 'scope of operational risk' and the 'scope of operational risk loss', in other words, on how events and losses pertinent to operational risk should be recognised within an institution's processes and businesses and how they should be treated for AMA capital purposes.

Article 4(52) of Regulation (EU) No 575/2013 defines operational risk as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events; this definition includes legal risk. However, the Regulation does not provide any further indication of the 'scope of operational risk' and the 'scope of operational risk loss', leaving the definitions open to different interpretations and allowing institutions to choose how they are implemented. This can have consequences in relation to operational risk regulatory capital and management practices as well as on supervisory assessment purposes, since institutions that have similar events and losses on operational risk may come up with significant differences in terms of operational risk profile and associated AMA regulatory capital.

With a view to ensuring uniform application across the European Union of the definition of operational risk established by Regulation (EU) No 575/2013 and avoiding inconsistencies in the determination of institutions' operational risk profile, these RTS clarify the scope of operational risk and the scope of operational risk loss. Competent authorities must refer to these criteria when assessing whether an institution AMA framework is effective in capturing and representing its operational risk profile.

Sound operational risk management is a reflection of the effectiveness of the management body and senior management in administering its portfolio of products, activities, processes and systems and is the foundation of an effective operational risk management framework. These RTS also specify common standards for the supervisory assessment of the governance of operational risk, in particular with respect to the role and responsibilities of the operational risk management function and the reporting system.

Article 322(2)(b) of Regulation (EU) No 575/2013 requires an institution adopting the AMA to use the four elements – internal loss data, external data, scenario analysis and business environment and internal control factors – as inputs to its operational risk measurement system. However, it does not clarify the manner in which these elements should be combined to calculate the AMA regulatory capital. Operational risk modelling is a relatively new and evolving discipline and each institution has a certain degree of flexibility in building its operational risk measurement system. However, this flexibility should not favour the development and implementation of ineffective, inconsistent or insufficiently risk sensitive internal risk models. These RTS set out standards for the supervisory assessment of key components of the operational risk measurement system, aimed at ensuring that the system is based on a well-founded methodology, effective at capturing

the institutions' actual and potential operational risk, reliable and robust in generating AMA regulatory capital requirements and comparable across institutions.

Unlike for other types of risk, the data relating to operational risk are not readily available, but need to be first identified within an institution's books and archives, and then properly gathered and maintained. Furthermore, the operational risk measurement system is typically very sophisticated and envisages several logical and computational steps for the generation of the AMA capital. In light of this, these RTS also establish criteria for supervisory assessment of an institution's data quality and IT systems.

Finally, these RTS set the criteria for supervisory assessment of the 'use test' requirement for operational risk envisaged by Article 321(a) of Regulation (EU) No 575/2013 and of the terms and scope of audit and internal validation reviews of the AMA framework.

## The nature of RTS under EU law

The draft RTS are produced in accordance with Article 10 of the EBA Regulation ([4]). According to Article 10(4) of the EBA Regulation, they will be adopted by means of regulations or decisions.

According to EU law, regulations are binding in their entirety and are directly applicable in all Member States. This means that, on the date of their entry into force, the regulations automatically become part of the national law of the Member States without the need for further enactment into national law.

Presenting these rules in the form of a draft Commission regulation should ensure a level-playing field by preventing divergent national interpretations in transposition, and thereby facilitating the cross-border provision of EU financial services.

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

# 4. Draft regulatory TS on assessment methodologies for the Advanced Measurement Approaches for operational risk under Article 312 (4) (a) of Regulation (EU) No 575/2013

Between the text of the draft RTS that follows, further explanations on specific aspects of the proposed text are occasionally given, which either offer examples or provide the rationale behind a provision, or set out specific questions for the consultation process. Where this is the case, this explanatory text appears in a framed text box.

**Contents**

**COMMISSION DELEGATED REGULATION (EU) No …/…**

**supplementing Regulation (EU) No 575/2013 of the European Parliament and of the Council by way of regulatory technical standards specifying the assessment methodologies for the Advanced Measurement Approaches for operational risk**

**of dd mmmm 201y**

THE EUROPEAN COMMISSION,

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

Having regard to Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012[5] , and in particular to Article 312(4), lett. (a) thereof,

Whereas:

1. For purposes of own funds requirements for operational risk, Article 312(2) of Regulation (EU) No 575/2013 provides competent authorities to permit an institution to use Advanced Measurement Approaches ('AMA') based on the institution's operational risk measurement system. Absent a clear indication, Article 312(2) should be understood to provide that the criteria for using AMA should be met by the institution at the moment of the application and on an on-going basis.
2. With the view to ensuring a uniform application across the European Union, Article 312(4)(a) of Regulation (EU) No 575/2013 mandates the EBA with developing regulatory technical standards specifying the assessment methodology according to which competent authorities permit an institution to use AMA.
3. The various elements concurring to define an institution's AMA framework should not be considered in isolation but rather reviewed and assessed as a package of interwoven elements, so that only an adequate level of compliance in each part of the framework can be considered satisfactory by the competent authorities.
4. In light of the definition of operational risk laid down in Article 4(1), point (52) of Regulation (EU) No 575/2013 and of the multifaceted peculiarity of operational risk, its correct identification and treatment for management and measurement, as well as for supervisory assessment purposes require that the scope of "operational risk" and the "scope of operational risk loss" be consistently applied throughout the Union. For this purpose appropriate standards should be set out for identifying and

[5] OJ…

treating operational risk events and losses wherever they may occur within an institution's organization.

5. Legal risk is included into the definition of operational risk, but no further indication is provided in Regulation (EU) No 575/2013 on how to identify operational risk events and losses driven by legal risk.

6. Moreover, since operational risk is inherent in all processes and businesses of an institution, it interacts with the other risk types to which these processes and business are exposed. Typically market risk and credit risk are the most important risk types where the boundary with operational risk occurs. When interacting with other risk types, operational risk is either the key driver of the loss or can contribute to amplify the loss primarily caused by the other risk types.

7. Article 322(3)(b) of Regulation (EU) No 575/2013, while requiring that all the operational risk losses that are related to market risk have to be included in the scope of the AMA capital calculation, does not provide further indication on how to identify and distinguish these losses from those, still occurring in market related activities, that do not bear any operational risk and as such should not be included into the scope of operational risk.

8. Moreover Article 322(3)(b) of Regulation (EU) No 575/2013 does not set out a clear-cut harmonised rule on the capital allocation of credit-related operational risk losses; rather the above mentioned provision limits itself to ensure that such losses are allocated alternatively to operational risk or to credit risk by providing that credit-related operational risk losses are excluded from the operational risk capital requirement, as long as the institution is required to continue to treat them as credit risk for the purpose of calculating minimum regulatory capital. With the view to ensuring a uniform application of such provision, it should be specified that certain operational risk losses caused by fraud events in the credit area should be included within the scope of operational risk for the purpose of calculating the AMA regulatory capital. Indeed in these cases the operational risk, rather than the credit risk, is the source of the origination of the credit position, and the loss generated by the operational risk event is strictly speaking a pure operational risk loss occurred in the credit process or credit product, rather than an operational risk loss related to credit risk (i.e. a boundary), as it might be in case of a collateral failure, legal defects or failure in credit process.

9. With the view to avoiding inconsistent interpretations of how operational risk reveals itself, consideration should be given to the fact that even though an operational risk loss can arise only from an operational risk event, its occurrence may be revealed by different items. Whilst some have a quantifiable impact and are reflected in the institution's financial statements, others are not quantifiable and do not affect the institution's financial statements and are therefore detectable from other sources such as managerial archives and incidents dataset.

10. The nature and quality of governance that directly or indirectly impacts on operational risk may affect both the institution's operational risk management decisions and the institution's qualification processes. In this regard, Regulation (EU) No 575/2013 prescribes certain guidance that should be addressed by the institution's governance and risk management framework.

11. The operational risk management function should play a key role in identifying, measuring and assessing, monitoring, controlling and mitigating the operational risks faced by the institution and it should be sufficiently independent from the institution's business units to ensure that its professional judgement and recommendations are both independent and impartial.

12. Senior management should be responsible for developing and implementing the operational risk governance and management framework that has been approved by the management body. Such framework should be consistently implemented throughout the institution's organisation, and all staff levels should be given adequate tools and information in order to understand their responsibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk in all material products, activities, processes and systems.

13. Art 76(5) of Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directive 2006/48/EC and 2006/49/EC [6] specifies that the risk management function has to ensure that all material risks are identified, measured and properly reported. With regard to operational risk, this entails that an institution should adopt effective risk reporting systems reflecting the up-to-date status of operational risk issues at the institution.

14. Effective internal reporting systems are a prerequisite of sound internal governance, they should be timely, accurate and complete and be made available not only to the management body and senior management but also to all the functions responsible for originating, identifying, assessing and measuring, monitoring, controlling and mitigating the operational risks which the institution is, or might be, exposed to.

15. AMA operational risk data can be grouped into the following four categories or elements: internal loss data, external data, scenario analysis and business environment and internal control factors. Article 322(2)(b) of Regulation (EU) No 575/2013 requires an institution adopting the AMA to use all these elements as inputs to its operational risk measurement system, however it does not clarify how these elements should be combined for calculating the AMA regulatory capital.

16. Operational risk modelling is a relatevely new and evolving discipline and it should be taken into account that for this reason Regulation (EU) No 575/2013 grants an institution significant flexibility in building the operational risk measurement system for calculating the AMA regulatory capital.

17. This flexibility, however, should not be conducive to significant differences across institutions in key components of the measurement system, such as the building of the calculation data set, the identification and determination of the severity and aggregate distributions, the incorporation of the capital offsets. With the view to ensuring that the risk measurement system is methodologically well founded, comparable across the institutions, effective in capturing the institutions' actual and potential operational risk and reliable and robust in generating AMA regulatory

[6] OJ L 176 of 27.6.2013, p. 338.

capital requirements, the methodology for AMA assessment should provide that the same criteria and requirements are applied by the competent authorities across the Union. The AMA assessment methodology should also adequately take into consideration the idiosyncratic components of operational risk that are related to the institutions' different size, nature and complexity.

18. Unlike other types of risks, the data relating to operational risk are not available at hand but need to be first identified within an institution's books and archives, and then properly gathered and maintaned. Furthermore, the measurement system is typically very sophisticated and envisages several logical and computational steps for the generation of the AMA capital. It is therefore crucial that data quality and IT systems are properly designed and correctly implemented within an institution so to serve the purpose for which they are built.

19. Pursuant to Article 321(a) of Regulation (EU) No 575/2013, an institution's internal operational risk measurement system has to be closely integrated into its day-to-day risk management processes. In light of this requirement, commonly referred to as the "use test", an AMA institution should ensure that its operational risk measurement system is not solely used for calculating regulatory capital, but is also integrated into its day-to-day business process, embedded within the consolidated entities and used for risk management purposes on an on-going basis. For the purpose of ensuring a consistent implementation of this requirement, the supervisory expectations to be met by an AMA institution as regards the "use test" should be adequately clarified.

20. Pursuant to Article 321(e) and (f) of Regulation (EU) No 575/2013, an AMA framework has to be subject to internal validation and audit reviews. The organisational structure of the audit and internal validation functions can vary depending on an institution's nature, complexity and operational risk profile. With the view to ensure consistency of the internal validation and audit reviews as well as their effectiveness and operational working, this Regulation lays down the supervisory assessment criteria governing the terms and scope of such reviews.

21. In order to provide both institutions and competent authorities with evidence that an institution operational risk measurement system is reliable and robust and generates a more credible operational risk own-funds requirement than the simpler operational risk regulatory methodology, it should be specified that parallel running for a certain period of time of the old and of the new model should be part of the AMA assessment.

22. The European Supervisory Authority (European Banking Authority) has conducted open public consultations on these draft regulatory technical standards, analysed the potential related costs and benefits and requested the opinion of the Banking Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1093/2010.

HAS ADOPTED THIS REGULATION:

## CHAPTER I

## GENERAL PROVISIONS

*Article 1*

*Scope of operational risk*

1. The competent authority shall verify that an institution has duly established and documented within its organization the scope of operational risk and operational risk loss in line with the definition set out in Art 4(1), point (52) of Regulation (EU) No 575/2013 and the interpretative criteria set out in Chapter II of this Regulation.

2. The competent authority shall verify that an institution has included legal risk, information and communication technology risks, as well as model risk, within the scope of operational risk with the exclusion of other kinds of risk.

*Article 2*

*Definitions*

For purposes of this Regulation the following definitions shall apply:

(1) 'AMA institution' means an institution being permitted to use or already using an AMA;

(2) 'calculation data set' means the portion of gathered data, either actual or constructed, that fulfils the necessary conditions to serve as input into the operational risk measurement system to generate the AMA regulatory capital;

(3) 'data collection threshold' means a loss value from which an institution identifies and collects operational risk losses for management and measurement purposes. The data collection threshold is usually determined by the inherent risk and complexity of the operational risk category, as well as by the cost benefit analysis of collecting the data below the threshold;

(4) ‘date of accounting or reserve’ means the date when a loss or reserve/provision was first recognized in the Profit and Loss statement (P&L), against an operational risk loss ;

(5) ‘date of discovery’ means the date on which an institution became aware of the operational risk event;

(6) ‘date of occurrence’ means the date when the operational risk event happened or first began;

(7) ‘*de minimis* modeling threshold’ means a loss value from which the frequency and severity distributions (either empirical or parametric) are fitted to the operational risk losses;

(8) ‘dependence’ means any form of dependence (e.g. linear or nonlinear, relating to all the data or just to the body or the tail) across two or more operational risk categories or within an operational risk category, that is caused by an institution’s internal and/or external factors. Dependence arises from exposures to common process, from structural factors (such as people, businesses processes, IT systems) or from environmental factors (such as a change in legal risk associated with certain business practices) that affect multiple areas of the institutions. These factors can influence the observed frequency or severity of losses within the institution;

(9) ‘gross loss’ means a loss stemming from an operational risk event or event type - as referred to in Article 322(3)(b) of Regulation (EU) No 575/2013 - before recoveries of any type;

(10) ‘information and communication technology risk’ means the risk of losses due to the inappropriateness or failure of the hardware and software of technical infrastructures, including risks compromising their availability, integrity, accessibility and the security of data.

(11) ‘IT infrastructure’ means the composite hardware, software, network resources and services required for the existence, operation and management of an IT environment. It allows an organization to deliver IT solutions and services to its employees, partners and/or customers and is usually internal to an organization and deployed within owned facilities. Typically, a standard IT infrastructure consists of the following components:

a. Hardware: Servers, computers, data centers, switches, hubs and routers, etc.
b. Software: Enterprise resource planning (ERP), customer relationship management (CRM), productivity applications and more.
c. Network: Network enablement, Internet connectivity, firewall and security.
d. Workers: individuals, such as network administrators (NA), developers, designers and generic end users with access to any IT appliance or service are also part of an IT infrastructure, specifically with the advent of user-centric IT service development.

(12) 'legal risk' means the risk of being sued or being the subject of a claim or proceedings due to non-compliance with legal or statutory responsibilities and/or to inaccurately drafted contracts. It also includes the exposure to newly enacted laws as well as to changes in interpretations of existing laws;

(13) 'near-misses' means operational risk events that do not lead to a loss, such as an IT disruption in the trading room just outside trading hours;

(14) 'operational risk category' means the level (such as the institution's organizational unit, operational risk event type, business line) at which the institution's operational risk measurement system generates a separate distribution for estimating potential operational losses. An operational risk category is homogeneous when its data are of the same or similar nature under the operational risk profile, independent when no form of dependence or correlation is identifiable across it, stationary when the characteristics of the data does not change when shifted in time or space;

(15) 'operational risk gains' means operational risk events that generate a gain;

(16) 'operational risk management' means the process of identifying, assessing, monitoring (including reporting), controlling and mitigating operational risks;

(17) 'operational risk measurement system' means the process to measure operational risk in order to determine the operational risk regulatory capital under an AMA**;**

(18) 'operational risk profile' means the representation at a given point in time of an institution's actual and prospective operational risk. Different inputs and sources can be used to build a view on an institution's operational risk profile, including risk tolerance statements, the four AMA elements (i.e. internal data, external data,

scenario analysis and business environment and internal control factors) and operational risk capital figures;

(19) 'opportunity costs/lost revenues' means operational risk events that prevent undetermined future business from being conducted, such as unbudgeted staff costs, forgone revenue, project costs related to improving processes;

(20) 'pending losses' means losses stemming from operational risk events, which are temporarily booked in transitory and/or suspense accounts and are not yet reflected in the P&L statement. The impact of some events, such as legal events, internal frauds, damage to physical assets, may be known and clearly identifiable before these events are recognized through the establishment of a reserve;

(21) 'recovery' means an independent occurrence related to the original operational risk loss that is separate in time, in which funds or inflows of economic benefits are received from a third party, such as insurers or other parties;

(22) 'operational risk appetite and tolerance' means a forward looking view of the aggregate level and types of operational risk that an institution is willing or prepared to incur which will not jeopardise its strategic objectives and business plan;

(23) 'operational risk appetite and tolerance statement' means an articulation in written form of the aggregate level of operational risk loss and event types that an institution is willing or prepared to incur in order to achieve its strategic objectives and business plan. It includes both qualitative and quantitative measures, such as thresholds and limits based on loss metrics;

(24) 'risk measure' means a single statistic extracted from the aggregated loss distribution at the desired confidence level, such as Value at Risk (VaR), or shortfall measures (e.g. Expected Shortfall, Median Shortfall);

(25) 'System Development Life Cycle' means a process for planning, creating, testing, and deploying an IT infrastructure;

(26) 'sub-exponential distribution' means a distribution whose tail decays slower than the exponential distribution. The class of sub-exponential distributions includes the Lognormal, Log-Gamma, Log-Logistic, Generalised Pareto, Burr, and Weibull (with shape parameter < 1). The Weibull (with shape parameter > 1) and Gamma distributions do not belong to the class of Sub-exponential distributions. Sub-

exponential distributions can better represent the shape of the data in the tail (other than their skewness in the body) by allowing estimates of parameters that do not depend on the higher order statistical moments;

(27) ‘timing losses’ means negative economic impacts booked in an accounting period due to operational risk events impacting the cash flows or financial statements of previous accounting periods. Timing impacts typically relate to the occurrence of operational risk events that result in the temporary distortion of an institution’s financial accounts (such as revenue overstatement, accounting errors and mark-to-market errors).

## CHAPTER II
## SCOPE OF OPERATIONAL RISK AND OPERATIONAL RISK LOSS

*Article 3*

*General principles*

1. The competent authority shall verify that an institution applies the criteria set out in Article 4 of this Regulation for purposes of identification and treatment of operational risk events and losses that are related to legal risk.

2. The competent authority shall verify that an institution applies the criteria set out in Article 5 of this Regulation for purposes of identification and treatment of operational risk events and losses that are related to market risk.

3. The competent authority shall verify that an institution applies the criteria set out in Article 6 of this Regulation for purposes of identification and treatment of fraud events and losses in the credit area.

4. The competent authority shall verify that an institution applies the criteria set out in Article 7 of this Regulation for purposes of identification and treatment of the loss items generated by an operational risk event.

*Article 4*

*Operational risk events related to legal risk*

1. The operational risk events related to legal risk, and the related losses, shall be included within the scope of operational risk for the purpose of calculating the AMA regulatory capital.

2. The definition in paragraph 1 shall include the following events:

    (a) events triggered by legal settlements - either judicial, or out of court, arbitration, claims negotiations - or from the voluntary decision of an institution to bear the loss so as to avoid an upcoming legal risk;

(b) events related to decisions made by an internal competent decision-maker but breaching legislative or regulatory rules, internal rules or ethical conduct.

3. As a specification of the paragraph 2, the following cases shall be included within the scope of application of paragraph 2, points (a) or (b):

(a) aggressive selling, such as those stemming from individual initiatives, with consequential breaches of legislative or regulatory rules, internal rules or ethical conduct;

(b) expenses stemming from legal disputes or from interpretations of legislative or regulatory rules which prove to be against industry practice;

(c) refunds (or discounts of future services) to customers caused by operational risk events, before the customers can lodge a complaint but after an institution has been required to refund other customers for the same event.

4. Events due to decisions or radical changes in the business environment, lack of responsiveness to changes in the business environment or improper implementation of decisions which did not breach any legislative or regulatory rules, internal rules or ethical conduct shall not be ascribed to operational risk.

5. As a specification of the paragraph 4, the following events, and the related losses, shall be excluded from the scope of operational risk:

(a) events incurred by an institution as a result of senior management's decisions or business choices, which do not breach any legislative or regulatory rule, internal rules or ethical conduct, or which are not triggered by legal risk;

(b) losses related to flawed investment choices in mergers or acquisitions, organizational or management restructuring;

(c) losses related to decisions made by an institution's competent decision making body, which are not compatible with the institution's risk tolerance level and deviate from its core business activities, in cases where these

decisions did not breach any legislative or regulatory rules internal rules or ethical conduct;

(d) refunds to customers and goodwill payments due to business opportunities, where no breach of legal or regulatory rules or ethical conduct have occurred. This applies only where the clients/counterparts are entirely at fault and an institution has fulfilled its obligations, such as reminding the clients or counterparts of their obligations on a timely basis.

*Article 5*

*Operational risk events related to market risk*

1. Operational risk events occurring in market-related activities shall be classified as boundary events between operational risk and market risk. These events, and the related losses, shall be included within the scope of operational risk for the purpose of calculating the AMA regulatory capital.

2. The definition in paragraph 5(1) shall include the following events:

   (a) events due to operational errors;

   (b) events due to failures in internal controls;

   (c) events due to wrong selection and/or implementation of the model, made outside a defined business process/formalised procedure and without a formalized, conscious risk-taking process; and

   (d) events due to inadequate data quality and unavailability of IT environment.

3. As a specification of the paragraph 5(2), the following cases shall be included within the scope of application of Article 5(2), points (a), (b), (c) or (d) respectively:

   (a) errors during the introduction or execution of orders;

   (b) errors in classification due to the software used by the front and middle office;

(c) incorrect specification of deals in the term-sheet, such as errors related to the transaction amount, maturities and financial features;

(d) loss of data and/or misunderstanding of the data flow from the front to the middle and back offices;

(e) technical unavailability of access to the market, for instance making it impossible to close contracts;

(f) failures in properly executing a stop loss;

(g) unauthorised market positions taken in excess of limits;

(h) selection of a model from a range of software without verifying its suitability for the financial instrument to be evaluated and for the current market conditions;

(i) errors in the IT implementation of a selected model; and

(j) incorrect mark-to-market valuations and VaR, due to erroneous booking of a trade into the trading system.

4. Events occurring in market-related activities which are the result of a deliberate corporate or investment decisions shall not be ascribed to operational risk.

5. As a specification of the paragraph 5(4), the following events, and the related losses, shall be excluded from the scope of operational risk:

(a) events due to wrong selection of a model, made through a formalized corporate process; and

(b) losses caused by a pricing model where the potential exposure to the model risk had been previously assessed.

**Explanatory Box**

For instance losses caused by pricing models, where the potential exposure to the model has been assessed by considering potential adjustments to "mark-to-market" transactions, have to be excluded from the scope of operational risk.

*Article 6*

*Fraud events in the credit area*

1. Operational risk events occurring in a credit product or credit process, which are caused by 'first party fraud' or 'third party fraud' shall be classified as fraud events in the credit area. These events, and the related losses, shall be included within the scope of operational risk for the purpose of calculating the AMA regulatory capital.

2. The definition in paragraph 6(1) shall include the following events:

   (a) lending decisions based on counterfeit documents or miss-stated financial statements, such as non-existence or over-estimation of collaterals and counterfeit salary confirmation;

   (b) fraudulent use of credit funds;

   (c) loan application fraud through phishing and using clients data;

   (d) loan application by client using fictitious identity;

   (e) fraudulent use of clients' credit cards by third parties.

**Explanatory Box**

Art. 322(3)(b) of Regulation (EU) No 575/2013 states that "An institution shall record the operational risk losses that are related to credit risk and that the institution has historically included in the internal credit risk databases in the operational risk databases and shall identify them separately. Such losses shall not be subject to the operational risk charge, provided that the institution is required to continue to treat them as credit risk for the purposes of calculating own funds requirements."

The RTS specifies that certain operational risk losses in the credit area are included within the scope of operational risk for the purpose of calculating the AMA regulatory capital. The current proposal takes a restrictive approach, providing that only losses that are caused by fraud events, either first party or third party, that generate a credit position (and loss) with a customer should be taken into account for AMA regulatory capital (see, for instance, the last sentence of 'first party fraud' definition). Indeed in

these cases the operational risk, rather than the credit risk, is the source of the origination of the credit position, and the loss generated by the operational risk event is technically speaking a pure operational risk loss occurred in the credit process or credit product, rather than an operational risk loss related to credit risk, as it might be in case of a credit risk loss due to a collateral failure, legal defects or failure in credit process.

Therefore these losses are not captured by Art 322(3)(b), of Regulation (EU) No 575/2013, but pertain fully to operational risk since, strictly speaking, they do not bear a credit risk. Furthermore, the sentence "the institution is required" does not entail a national discretion and leaves room for the EBA to provide pertinent implementation standards of this provision.

Complexities in distinguishing some fraud events ex-ante or even ex-post had originally led institutions to include these losses in credit risk databases, especially when operational risk did not exist as an autonomous risk category for regulatory purposes. With the implementation of the EU Directive 2006/48/, which contained the same provision, AMA institutions started to identify these losses and to record them separately in operational risk databases. Some of these institutions have moved forward by including them in AMA capital calculation. Indeed these losses, if included in credit risk model, could bias not only PD and LGD figures but also pricing process and results for lending products, with the consequence of charging on customers costs and expenses related to an institution internal inefficiency rather than customers' creditworthiness.

The current practice of dealing with these events and losses for regulatory purposes is therefore very diversified, with some institutions that include all fraud events emerged in the credit area into the AMA capital calculation, other institutions that include only third party frauds, others that do not include any fraud events into the AMA.

These RTS aim at providing clarity on this topic, by setting a clear line between the pure operational risk events (and losses) that occur in the credit area (i.e. fraud events) and the true boundaries, with the view of harmonizing the practices and reducing the areas of inconsistencies. Unlike this specific case, all the other credit risk losses generated by operational risk events are considered boundary losses between operational risk and credit risk and fall within the scope of application of Art 322(3)(b) of Regulation (EU) No 575/2013.

To ease the implementation of this provision, a phase-in approach is proposed for AMA capital calculation.

3. The competent authority shall verify that the institution adjusts the data collection threshold relating to the loss events described in Article 6(1) up to levels consistent with those adopted for the collection of the loss events pertinent to the other operational risk categories of the AMA framework.

**Explanatory Box**

Usually institutions operate thresholds for collecting in the operational risk database frauds in a credit product or credit process. These thresholds vary between institutions and may also vary between products of the same institution (for example the threshold for fraud in relation to credit cards may be smaller than it is for other products). Generally these thresholds are much higher of those adopted for the collection of the rest of operational risk events.
Given the current differences within and between institutions and the costs of implementing a lower data collection threshold for these events, a phase in approach is proposed to permit institution to

achieve consistency in threshold-setting and data gathering between fraud events in the credit area and all other operational risk events.

4. For the purpose of this provision:

(1) 'first party fraud' means a fraud that is committed by an individual or group of individuals on their own account with no intention of any repayment of the loss caused. A first party fraud generally occurs when the party misrepresents its financial abilities on the application forms and by using another person's identifying information. Any fraud which is initiated at a later stage of the lifecycle of a credit product, such as the misstatement of financial reports, even when it is used to prolong or to extend an existing credit product does not fall within this definition;

(2) 'third party fraud' means a fraud that is committed by means of use of a person's identity, such as the use of false identification documents, without the knowledge of the person whose identity is used to commit the fraud. The fraudster can be an individual without a business relationship with the institution (external fraud) or an employee (internal fraud) and can involve existing client relationships (client is unaware) or new client relationships (real identity of client is unknown). If there is any active involvement of an existing client in the fraud, this is treated as first party fraud.

*Article 7*

*Scope of operational risk loss*

1. For the purpose of calculating the AMA regulatory capital, the scope of operational risk loss shall include the following items:

(a) direct charges (including impairments) to the P&L and write-downs due to the operational risk event;

(b) costs incurred as a consequence of the operational risk event that include:

(1) external expenses with a direct link to the operational risk event, such as legal expenses directly related to the event and fees paid to advisors, attorneys or suppliers;

(2) costs of repair or replacement to restore the position that was prevailing before the operational risk event;

(c) provisions or reserves accounted for in the P&L against potential operational losses;

(d) pending losses that are recognised to have a relevant impact. Pending losses shall be included within a time period commensurate to the size and age of the pending item. For this purpose, consideration shall be given to the recognition of pending losses actual amount in the loss database or pertinent scenario analysis;

(e) uncollected revenues related to contractual obligations with third parties, such as the decision to compensate a client following the operational risk event, rather than by a reimburse or direct payment, through a revenue adjustment waiving or reducing contractual fees for a specific future period of time;

(f) timing losses that span more than one accounting year and give rise to legal risks.

2. An institution shall record and use, at least for AMA management purposes, the following additional items when they originate from a relevant operational risk event:

(a) near-misses;

(b) operational risk gains;

(c) opportunity costs/lost revenues;

(d) internal costs such as overtime or bonuses.

3. The following items shall be excluded from the scope of operational risk loss:

(a) costs of general maintenance contracts on property, plant or equipment;

(b) internal or external expenditures to enhance the business after the occurrence of an operational risk event such as upgrades, improvements, risk assessment initiatives and enhancements;

(c) insurance premiums.

*Article 8*

*Recorded loss amount of the operational risk items*

1. The whole amount of the incurred loss or expenses shall be included in the scope of operational risk loss according to Article 7(1). This includes:

   (a) all the expenses incurred as a result of the operational risk event, such as provisions, costs of settlement, amounts paid to make good the damage, penalties, interest in arrears and legal fees;

   (b) in case of operational risk events related to market risk, the costs to unwind market positions, unless the position is intentionally kept open after the operational risk event is recognized. In the latter case, any portion of the loss due to adverse market conditions after the decision to keep the position open shall be ascribed to market risk;

   (c) in case of tax payments related to failures and/or inadequate processes, the expenses incurred as a result of the operational risk event, such as penalties, interest/late-payment charges, legal fees, with the exclusion of the tax amount originally due;

   (d) in case of fraud events in the credit area, the total outstanding amount at the time or after the discovery of the fraud (whole write-off amount, total credit loss) and any other related expenses, such as interest in arrears and legal fees.

2. In case of rapidly recovered loss events, an institution may consider that only the loss net of the rapid recovery constitutes the loss to be included into the scope of

operational risk loss. When the whole loss is rapidly recovered, the event is considered to be a near miss according to Article 7(2)(a) of this Regulation. For purposes of this Article 8, 'rapidly recovered loss events' means operational risk events that lead to losses that are recovered within five working days.

3. In case of timing losses, the loss amount to be recorded comprises all the expenses incurred as a result of the operational risk event, including the correction of the financial statement, when it involves the direct relation with third parties (such as customers or authorities) or employees of the institution, and excluding the correction of the financial statement in all other cases.

**Explanatory Box**

Examples of cases with timing losses and identification of operational risk loss amount:

i) Due to a procedural error or aggressive selling, for three years a customer is charged with higher than contracted fees/interests, which determine the revenue overstatement of the institution financial statement. After receiving the claim, the institution refunds the customer of the extra fees/interests; the institution also bears legal expenses and pays a fine to the competent authority. The loss amounts to be included in the scope of operational risk loss are the extra fees/interests, the legal expenses and the fine.

ii) In a dispute with an employee for mobbing, an institution is convicted by the court to refund the employee of the unpaid income/salary during five years. The institution also bears legal expenses and pays a fine. The loss amounts to be included in the scope of operational risk loss are the unpaid income/salary, the legal expenses and the fine.

iii) An operational risk event, such as an accounting or a mark-to-market error, occurs in an institution's portfolio determining the revenue overstatement of the institution's financial statements for three years. After three years the institution recognizes the operational risk event and corrects the financial statement. Due to this event the institution is fined by the competent authorities, an action for collective redress is filed (e.g. as a consequence of a fallen share price) and a provision is made. As the operational risk event does not directly involve a third party or an employee, the loss amounts to be included in the scope of operational risk loss are the fines and the provisions only. The restatement is not included in the scope of operational risk loss.

## CHAPTER III

## OPERATIONAL RISK MANAGEMENT

*Article 9*

*Documentation*

The competent authority shall verify that an institution has set up a complete and appropriate documentation on the criteria, processes, methodologies, applications and systems, including IT infrastructure, of the AMA framework, as well as on all elements of the operational risk governance and operational risk management.

*Article 10*

*Governance structure*

1. The competent authority shall verify all the parts of the AMA framework in order to evaluate that, in respect of operational risk, the governance arrangements of an institution as referred to in Articles 74(1), 76(2), 76(3), 76(4) and 85(1) of Directive 2013/36/EU and in Article 321(1), letters (b), (c) and (d) of Regulation (EU) No 575/2013, are satisfactorily complied with for the use of AMA. The competent authority shall verify that:

    (a) the operational risk management standards employed by the institution are appropriate and sufficient;

    (b) the operational risk management function is independent;

    (c) the senior management involvement with operational risk is active and consistent; and

    (d) the reporting of the operational risk profile and of the management of operational risk is regular, timely and sufficient and includes all material aspects of operational risk management and measurement.

2. In performing the assessment mentioned in this Article 10, the competent authority shall verify the governance structure as a whole and shall not verify the individual parts separately from each other.

3. The competent authority shall verify that an institution has a clear organisational structure for the governance and management of operational risk with well defined, transparent and consistent lines of responsibility taking into account the nature, scale and complexity of the activities of the institution.

**Explanatory Box**

For example, it is unlikely that an institution with an adequate operational risk governance and risk management structure but with weaknesses in other AMA elements could be perceived to have an acceptable AMA framework. In addition, weaknesses in one area may well make it impossible for an institution to implement a successful element elsewhere. For example, an institution with poor reporting and management information is unlikely to have an effective governance structure.

*Article 11*

*Operational risk governance and management*

1. The competent authority shall evaluate the effectiveness of an institution's operational risk governance and management framework on the basis of their impact on behaviour, engagement in operational risk management and culture. The competent authority shall focus on:

   (a) awareness of staff;

   (b) operational risk culture;

   (c) internal challenge process.

2. For purposes of Article 11(1), the competent authority shall verify that:

   (a) the institution's management body discusses and approves the operational risk governance and management framework including policies, processes, controls and systems through which operational risk is identified, assessed and measured, monitored/reported, controlled and mitigated for AMA regulatory purposes;

(b) at least on an annual basis an institution's management body discusses and approves the operational risk appetite and tolerance statement, ensuring that it is clear and understood throughout the institution;

(c) an institution's management body monitors on a continuous basis the institution's performance against the operational risk appetite and tolerance statement;

**Explanatory Box**

The effectiveness and authority of an operational risk governance and management framework is often reliant on the cultural 'tone-setting' from the management body and senior management, which should be evidenced by their behaviours and communications, for example, the promotion of a 'no blame' culture for reporting actual risks losses and near misses throughout the organisation. The operational risk function benefits when senior management fully endorse, deploy, review and uphold the firm's procedures and outcomes for identification, assessment/measurement, monitoring and reporting, controlling and mitigating operational risk.

(d) an institution ensures that there is an on-going process to identify, assess and measure, monitor and report operational risk and that it is able to identify the responsible staff for all parts of this process;

(e) an institution ensures that the information from the process indicated in point (d) above goes to the relevant committees and executive bodies and that any decision arising from these committees is duly communicated to those areas within the institution that collect, control and monitor operational risk and those that manage activities that give rise to operational risk;

(f) an institution ensures that there is a regular evaluation of the effectiveness of the operational risk governance and risk management arrangements and notifies the relevant competent authority of its findings. Such evaluation and pertinent notification shall be carried out on at least an annual basis.

**Explanatory Box**

Awareness of staff - Every member of staff has an important role to play in the management and mitigation of operational risk within an institution. Supervisors should investigate if staff is aware of their responsibilities with regard to identifying, managing, monitoring and reporting operational risks. Institutions could elect to raise awareness of operational risk among staff and embed the operational risk framework into the day-to-day risk management process of the institution.

Culture - A strong risk culture, running through the entire organization is a prerequisite. For example, it should be better to 'own up' than hide an error, if a no blame culture exists. Such cultures are difficult to achieve without the direct, active and demonstrable sponsorship and support of the management body and senior management. A favorable culture is also likely to be achieved if business units are engaged with the governance structure and do not view the arrangements as a constraint.

Challenge - One of the key components of an effective governance structure is challenge throughout the structure – including at management body, senior management and committee level. Various mechanisms should exist to enable firms to judge the quality and effectiveness of the challenge process – including committee minutes and notes for record.

Supervisors should use a 'vertical slice' through the operational risk governance and risk management framework to help understand the workings of the processes and procedures, behaviours, engagement and the institution's risk culture. This may show how risks and events are escalated within the governance structure and involves tracking the reporting, review and response to a significant operational risk event, from its discovery in a business unit up to the management body or most senior risk committee in the firm. Examining the 'vertical slice' could extend to considering how any responses, reactions and decisions are communicated to the original business unit.

*Article 12*

*Independent operational risk management function*

1. The competent authority shall verify that an institution's operational risk management function is independent from the institution's business units. For this purpose, the competent authority shall verify that the operational risk management function undertakes, if relevant, the following tasks: oversight of the operational risk framework; analysis of the operational risk associated with the introduction and development of new products, markets, lines of business, processes, systems and significant changes to existing products; and an appropriate involvement in exceptional transactions.

**Explanatory Box**

The approval process of a new 'product' should consider the adequacy of the tools and expertise of the operational risk management, information technology, business line and internal control functions to identify, manage, monitor and report the resultant operational risk.

Operational risk arising from mergers and acquisitions could be assessed in a similar way. This is particularly important given the confidentiality and timeframe within which mergers and acquisitions are negotiated and the complicated nature of the process.

2. The competent authority shall verify that the operational risk management function is (i) empowered and supported by the management body and senior management; (ii) independent of business lines; (iii) not responsible for the audit function, taking into account the audit function's role in challenging the operational risk framework.

3. The competent authority shall also verify that the head of the operational risk management function is:

   (a) appropriately experienced for the operational risk profile;

   (b) in regular contact with the management body and its committees, depending on the delegation of authority and the risk management structure of the institutions;

   (c) actively involved in the elaboration of an institution's operational risk appetite and tolerance as well as in the strategy for its management and mitigation;

   (d) independent from the operational units and functions reviewed by the operational risk management function;

   (e) allocated a budget for the operational risk management function by the chief risk officer or a sponsoring member of the management body in a supervisory capacity and not by a business unit or executive function.

*Article 13*

*Senior management involvement*

The competent authority shall verify that an institution ensures that the senior management is responsible for implementing the operational risk governance and management framework approved by the management body, and has been delegated the responsibility by the management body, for developing policies, processes and procedures for managing operational risk.

**Explanatory Box**

For purposes of undertaking the above-mentioned tasks, the requirements placed on the senior management may include in particular:

a. translating the management body-approved operational risk management framework into specific policies, processes and procedures that can be implemented and verified within the different business units;

b. managing operational risks on regular basis, under the oversight of the management body;

c. implementing the operational risk framework through the institution;

d. developing and obtaining approval for policies, processes and procedures for managing and approving operational risk in all new and material products, processes and systems;

e. articulating and gain board approval for what constitutes the institutions' operational risk appetite and tolerance as well its strategy for the management and mitigation of operational risk;

f. possessing a good understanding of the institution's AMA and its operation, making sure that:

(i). all activities which can give rise to operational risk are conducted by staff with necessary experience, technical capability and resources;

(ii). the operational risk management policy is clearly and appropriately communicated to staff in all units;

(iii). remuneration policies are consistent with the institutions' appetite and tolerance for operational risk, as expressed in the operational risk appetite and tolerance statement; and

(iv). operational risk staff communicate effectively with staff responsible for credit risk, market risk, compliance and other risks, insurance purchasers and outsourcing arrangers

g. having a full understanding of the nature of the business and activities of the institution. The approval process of a new 'product' should consider the adequacy of the tools and expertise of the operational risk management, information technology, business line and internal control functions to identify, manage, monitor and report the resultant operational risk.

*Article 14*

*Reporting*

1. The competent authority shall verify the timeliness, accuracy, and relevance of an institution's reporting systems and internal controls and shall verify that the institution's operational risk reports fully reflect identified problem areas and if they motivate timely corrective action of outstanding issues. For these purposes the competent authority shall verify that:

   (a) the institution ensures that the reports are distributed to appropriate levels of management and to areas of the institution which the reports have identified as an area of concern and other relevant areas;

   (b) the institution's senior management receives at least quarterly reports, reflecting the up-to-date status of the institution's operational risk profile and shall use these reports in the decision making process;

   (c) the institution's operational risk reports contain relevant management information and that they include at least a high-level summary of the top operational risks of the institution and of the relevant subsidiaries and/or business units;

   (d) the institution uses ad hoc reports in case of certain deficiencies in the policies, processes and procedures for managing operational risk because promptly detecting and addressing these deficiencies can substantially reduce the potential frequency and/or severity of a loss event.

**Explanatory Box**

The operational risk reports may contain internal financial, operational, and compliance data, as well as external market information about events and conditions that are relevant to decision-making.

Management information needs to be in a form that the users can readily understand, challenge and act on. It can be useful, for example, to have a high-level summary of the top risks at the firm

in the form of a risk dashboard. The provision of a heat map summary of their risk ranking, which shows risks of higher or lower frequency and of higher and lower severity. This type of report can be developed for each business area as well as the institution as a whole and can be supported by underlying reports providing more detail. It can be important for the reports to identify in a clear and easy-to-understand manner any concentration of risks that might pose a threat to the business and reasons for any movements in risk rankings.

Besides loss data and scenario analysis, Key Risk Indicator (KRI) trend analysis can be informative to detect current and future areas exposed to operational risk. The appropriate aggregation of KRIs when amassing data upwards from smaller business areas to larger regional areas is important; for example, it may be beneficial that senior management challenge KRI data that never changes as this may mean that the KRI is not measuring true areas of risk, thresholds are not set at the correct level or controls may be continually failing.

## CHAPTER IV

## OPERATIONAL RISK MEASUREMENT

### Section I - The four AMA elements

*Article 15*

*General principles*

1. The competent authority shall verify that an institution groups AMA operational risk data into the following four elements: internal loss data, external data, scenario analysis and business environment and internal control factors.

2. The competent authority shall verify that an institution has internal documentation specifying in detail how the four elements are gathered, combined and/or weighted. The documentation shall also include a description of process modeling that illustrates the use and combination of the four elements and of the rationale for the modeling choices.

3. The competent authority shall verify that an institution has a clear understanding of how each of the four data elements influences the AMA regulatory capital. An

institution shall also be able to illustrate that the combination of the four elements is based on a sound statistical methodology, sufficient for estimating high percentiles.

4. The competent authority shall verify that an institution applies the criteria set out in Articles from 16 to 19 of this Regulation for the collection or generation and treatment of the four elements.

*Article 16*

*Internal loss data*

1. Following an operational risk event and with the exception of when the gross loss is rapidly recovered (as laid down in Article 8(2) of this Regulation), an institution shall be able to separately identify the gross loss amount as well as insurance recoveries and recoveries except insurance. For this purpose an institution shall adopt clear and consistent definitions within the group of "gross loss", "insurance recoveries" and "recoveries except insurance".

2. A system for defining and justifying appropriate thresholds - based on the gross loss amount - for each operational risk category, both for data collection (data collection threshold) and modeling (*de minimis* modeling threshold) shall be implemented.

3. The data collection threshold(s) selected by an institution for the operational risk categories shall be reasonable and shall not omit loss event data that are material for effective operational risk measurement and risk management.

4. For each individual operational loss, an institution shall be able to identify and record in the internal database, at least, the date of occurrence (when available), the date of the discovery and the date of accounting or reserve.

*Article 17*

*External loss data*

1. The competent authority shall verify that an institution that participates in consortia initiatives for the collection of operational risk events and losses shall provide data of comparable quality, as to scope, integrity and comprehensiveness, to the internal data

standards set out in Article 16. Information obtained from consortia initiatives which have the abovementioned characteristics are an appropriate external data source for AMA capital calculation.

2. The competent authority shall verify that an institution shall have a data filtering process in place which involves the selection of relevant external data, based on specific established criteria and that it is necessary to ensure that the external data being used is relevant and consistent with the risk profile of the institution. To avoid bias in parameter estimates, the filtering process shall result in consistent selection of data regardless of its loss amount; furthermore, if an institution permits exceptions to this selection process, it shall have a policy providing criteria for exceptions and documentation supporting the rationale for any exceptions.

3. For the purposes of the paragraphs (1) and (2), an institution, if needed, shall adopt a data scaling process involving the adjustment of loss amounts reported in external data to fit the institution's business activities, nature and risk profile. In such cases, the scaling process shall be systematic and statistically supported and shall provide outputs that are consistent with the institution's risk profile. The institution's scaling process shall be consistent over time and its appropriateness shall be regularly reviewed.

*Article 18*

*Scenario analysis*

1. For AMA purposes, the use of scenario analysis is not restricted to evaluating exposures to high severity events. In certain approaches or cases, scenarios may be used to provide information on the institutions overall operational risk exposure.

2. The competent authority shall verify that an institution ensures a robust governance framework impacting the scenario process in order to generate credible and reliable estimates regardless of whether or not the scenario is used for evaluating high severity events. For this purpose, the competent authority shall verify that:

    (a) the scenario process shall be clearly defined, well documented, repeatable and designed to reduce as much as possible subjectivity and biases, including anchoring, availability and motivational biases;

(b) qualified and experienced facilitators shall provide consistency in the process;

(c) the assumptions used in the scenario process shall be based to the maximum extent on the relevant internal data and external data with a structured selection process;

(d) the chosen number of scenarios, the level at (or units in) which scenarios are studied shall be rational and explained. The scenario estimates shall take into account relevant changes in the internal and/or external environments that can affect the institution's operational risk exposure. Business Environment and Internal Control Factors ('BE&ICFs') can be informative and useful for constructing scenario data.

(e) the scenario process and estimates shall be subject to a robust independent challenge process and oversight.

*Article 19*

*Business Environment and Internal Control Factors*

1. The BE&ICFs shall be forward looking and shall reflect potential sources of operational risk such as rapid growth, the introduction of new products, employees turnover and system downtime.

**Explanatory Box**

BE&ICFs can be incorporated into the AMA model in different ways, such as an indirect input into the quantification framework or as an ex-post adjustment to model output. Ex-post adjustments serve as an important link between the risk management and risk measurement processes and may result in an increase or decrease in the AMA capital charge at the group-wide or business-line level.

Potential sources of operational risk are those factors that affect the institutions risk profile. They are often, but not limited to, defined as risk drivers in the institutions Key Risk Indicators. Additional examples to those listed above are: frequent reorganizations, ineffective controls, poor process design or execution, entering new markets, key employee dependencies, the introduction of new IT systems or changes in IT environment and legal environment.

2. Given the subjective nature of BE&ICF adjustments, an institution shall have clear policy guidelines that limit the magnitude of either positive or negative adjustments as well as a policy to handle situations where the adjustments actually exceed these limits based on the current BE&ICFs.

3. The BE&ICF adjustments shall be well supported. Over time, the direction and magnitude of adjustments shall be compared to internal loss data, conditions in the business environment and changes in the validated effectiveness of controls to ensure appropriateness.

4. The level of supervisory scrutiny shall increase with the size of the adjustments due to BE&ICFs.

## Section II – AMA modeling assumptions

*Article 20*

*General principles*

The competent authority shall verify that an institution applies the criteria set out in Articles from 21 to 23 of this Regulation for the development, implementation and maintenance of an operational risk measurement system that is methodologically well founded, effective in capturing the institution's actual and potential operational risk, and reliable and robust in generating AMA regulatory capitals.

**Explanatory Box**

Across the EU there is a wide variety of approaches to AMA modelling. These include the Loss Distribution Approach (LDA) and the Scenario Based Approach (SBA). While LDA models tend to be built on actual loss data and SBA approaches usually rely on constructed (i.e. scenario generated) data, in practice the two methods usually overlap. Hybrid approaches are commonly found, with actual loss data often enriched by constructed data and vice versa. Thus, while some of the criteria in the following paragraphs are more applicable to one approach than another (and this does not only mean LDA or SBA), the underlying concepts and principles are meant to be generally valid and should therefore be applicable to any AMA approach.

*Article 21*

*Building the calculation data set*

1. The competent authority shall verify that an institution has a policy that identifies when an event or loss recorded in the internal loss events database is also to be included in the calculation data set. For this purpose specific criteria and examples shall also be defined by the institution for the classification and treatment of these events and losses within the calculation data set. This policy shall provide a consistent treatment of loss data across the institutions.

2. The competent authority shall verify that an institution uses alternatively "gross loss amount" or "gross loss amount after all recoveries (except insurance)" in the calculation data set. The competent authority shall verify that an institution does not use loss net of insurance recoveries in the calculation data set.

3. The competent authority shall verify that, for operational risk categories with low frequency of events, an observation period greater than five years is adopted in order to ensure sufficient data to generate reliable operational risk measures.

4. The competent authority shall verify that an institution uses the date of discovery or the date of accounting for building the calculation dataset. The competent authority shall verify that an institution uses a date no later than the date of accounting or reserve for including legal related losses or provisions into the calculation dataset.

5. The competent authority shall verify that the choice of *de minimis* modeling threshold does not adversely impact the accuracy of the operational risk measures. In particular, the use of *de minimis* modeling thresholds that are much higher than the data collection thresholds shall be limited and, when established, properly justified by sensitivity analysis at various thresholds. All operational losses above the set modelling threshold(s) shall be included in the calculation dataset and used, whatever their amounts, for generating the AMA regulatory measures.

6. The competent authority shall verify that an institution considers applying appropriate adjustment rates on data when inflation or deflation effects are material.

7. The competent authority shall verify that losses caused by a common operational risk event or by multiple events linked to a single root-event are grouped and entered into the calculation dataset as a single loss. The competent authority shall verify that possible exceptions are documented and properly addressed to prevent undue reduction of the capital figures.

8. The competent authority shall verify that an institution ensures that loss adjustments of single or linked events are not discarded from the AMA calculation data set in the case that the reference date of these adjustments falls inside the observation period and the reference date of the initial (single or root) event falls outside such a period.

9. The competent authority shall verify that an institution shall be able to distinguish for each reference year included in the observation period the loss amounts pertinent to events discovered (accounted) in that year from the loss amounts pertinent to adjustments or grouping of events discovered (accounted) in previous years.

10. For purposes of this Article, 'root event' means the initial operational risk event from which related events have been generated and/or pertinent losses emerged.

*Article 22*

*Granularity*

1. The competent authority shall verify that an institution takes into account the nature, complexity and idiosyncrasies of its business activities and the operational risks which it is exposed to, with the view to grouping together risks sharing common factors and defining the operational risk categories of an AMA.

2. For purposes of Article 22(1), the competent authority shall verify that an institution supports its choice of granularity by qualitative and quantitative means. An institution shall strive to get operational risk categories with homogeneous, independent and stationary data.

3. The competent authority shall verify that an institution provides evidence that its choice of operational risk categories is reasonable and does not adversely impact the conservatism of the model outcome or of its parts.

4. The competent authority shall verify that an institution ensures that the choice of granularity remains valid on a regular basis.

*Article 23*

*Identification of the probability distributions*

1. The competent authority shall verify that an institution follows a well specified, documented and traceable process for the selection, update and review of probability distributions and the estimate of their parameters. This process shall result in consistent and clear choices by the institution and shall be finalised with the view to properly capture the risk profile in the tail.

2. The competent authority shall verify that the following steps are included in the process for the selection of the probability distributions:

    a. Exploratory Data Analysis ('EDA') for each operational risk category to better understand the statistical profile of the data and select the most suitable distribution;

    b. appropriate techniques for the estimation of the distributions parameters; and

    c. appropriate diagnostic tools for evaluating the appropriateness of the distributions to the data, giving preference to those most sensitive to the tail.

    For the purposes of this provision, Exploratory Data Analysis (EDA) is the process of using statistical tools, such as graphs, measures of center, variation, skewness and leptokurtosis to investigate data sets in order to understand their main characteristics.

3. The competent authority shall verify that an institution pays particular attention to the positive skewness and leptokurtosis of the data when selecting a severity distribution. When the data are much dispersed in the tail, empirical curves shall not be used to estimate the tail region. Sub-exponential distributions shall be used for this purpose unless there exist exceptional reasons to apply other functions, which shall be in any case properly addressed and fully justified to prevent undue reduction of the capital figures.

4. When separate distributions for the body and the tail are used, the competent authority shall verify that an institution carefully considers the choice of the body-tail modelling threshold that distinguishes the two regions. Documented statistical support, supplemented as appropriate by qualitative elements, shall be provided for the selected threshold, as the threshold choice may significantly impact the capital requirements.

   For purposes of this Article 23, 'body-tail modelling threshold' means a loss value that separates the body from the tail of the loss distributions and that may generate the adoption of a separate distribution for estimating potential losses.

5. When estimating the parameters of the distribution, the competent authority shall verify that an institution takes into account the incompleteness of the calculation dataset in the model due to the presence of *de minimis* modeling threshold(s). The competent authority shall verify that an institution provides evidence that an incomplete calculation dataset does not adversely impact the accuracy of the parameter estimates and capital requirements.

6. The competent authority shall verify that an institution pays particular attention to the estimate of the kurtosis-related parameters, which describe the tail region of the losses and can be unstable when data are scarce. The competent authority shall verify that an institution shall put in place methodologies to reduce estimate variability and provide measures of the error around these estimates such as confidence intervals and p-values.

7. The competent authority shall verify that, when an institution adopts robust estimators, it can demonstrate that their use does not underestimate the risk in the tail.

For the purpose of this provision 'robust estimators' means a generalization of classical estimators such as the Maximum Likelihood or Probability Weighted Moments, which have still good statistical properties (e.g. high efficiency, low bias) for a whole neighborhood of the unknown underlying distribution of the data. These estimators may also be used as a diagnostic technique for evaluating the sensitivity of the capital charge to the chosen parameter estimation method.

8. The competent authority shall verify that an institution assesses the goodness-of-fit between the data and the selected distribution by using diagnostic tools (both graphical

and quantitative) which are more sensitive to the tail than to the body of the data, especially when the data are very dispersed in the tail. When appropriate, for instance when the diagnostic tools do not lead to a clear choice of the best-fitting distribution or to mitigate the effect of the sample size and the number of estimated parameters in the goodness-of-fit tests, evaluation methods that compare the relative performance of the distributions shall be used.

**Explanatory Box**

Examples of evaluation methods to assess the relative performance of the distributions include the Likelihood Ratio, the Akaike Information Criterion, the Schwarz Bayesian Criterion.

9. The competent authority shall verify that an institution has a regular cycle to control assumptions underlying the selected probability distributions. If assumptions are invalidated, for instance because they generate values outside established ranges, alternative methods shall be tested and any change shall be properly justified and implemented, in accordance with the EBA/RTS/6/2013.

*Article 24*

*Determination of aggregated loss distributions and risk measures*

1. The competent authority shall verify that the techniques elaborated by an institution to determine the aggregated loss distributions ensure appropriate levels of precision and stability of the risk measures. The risk measures shall be supplemented with information on their level of accuracy.

2. An institution may use several statistical techniques to generate the aggregated loss distributions from frequency and severity curves and parameter estimates, such as Monte Carlo simulations, Fourier Transform-related methods, Panjer algorithm and Single Loss Approximations. Regardless of the techniques used to aggregate frequency and severity distributions, the competent authority shall verify that an institution adopts criteria that mitigate sample and/or numerical related errors and provides a measure of the magnitude of these errors.

3. Where Monte Carlo simulations are used, the number of steps to be performed shall be consistent with the shape of the distributions and with the confidence level to be achieved. Where the distribution of losses is heavy tailed and measured at a high confidence level, the number of steps shall be sufficiently large to reduce sampling variability to an acceptable level. If Fourier Transform or other numerical methods are used, attention shall be paid to algorithm stability and error propagation issues.

4. The competent authority shall verify that an institution ensures that the risk measure generated by the operational risk measurement system: (i) fulfils the monotonic principle of risk, which can be seen in the generation of higher (lower) capital requirements when the underlying risk profile increases (decreases) and (ii) is realistic from a managerial and economical perspective. For this purpose, the competent authority shall verify that the institution applies appropriate techniques to avoid:

    (a) capping the maximum single loss;

    (b) implying the non-existence of the first moment, as this would determine high capital requirements and would not be easily and clearly justifiable and applicable within organizations.

5. The competent authority shall verify that an institution explicitly evaluates the robustness of the outcome of the operational risk measurement system by performing appropriate sensitivity analysis on the input data and/or its parameters.

## Section III – Expected losses and dependence

*Article 25*

*Expected losses*

1. The competent authority shall verify that an institution meets the criteria set out in this Article in order to calculate the AMA regulatory capital only on unexpected losses ('UL'), as provided for in Article 322(2), lett. (a) of Regulation (EU) No 575/2013, and

to assess whether the expected loss ('EL') is adequately captured in the institution's internal business practices.

2. The competent authority shall verify that an institution's estimate of EL is consistent with the EL plus UL regulatory capital calculated using the operational risk measurement system. The EL estimation process shall be done by operational risk category and shall be consistent over time.

3. The competent authority shall verify that an institution defines the EL by using statistics that are less influenced by extreme losses, such as median and trimmed mean, especially in the case of medium/heavy tailed data. The maximum offset for EL shall be bounded by the total EL and, in each operational risk category, by the pertinent EL calculated according to the institution's operational risk measurement system applied to that category.

4. The competent authority shall verify that allowable offsets for EL in each operational risk category are clear capital substitutes or otherwise available to cover EL with a high degree of certainty over a one year time horizon. Where the offset is something other than provisions, its availability shall be limited to those operations with highly predictable, reasonable stable, routine losses. Because exceptional operational risk losses do not fall within EL, specific reserves for any such events that have already occurred shall not qualify as allowable EL offsets.

5. The competent authority shall verify that an institution clearly documents how its EL is measured and captured, including how any EL offsets meet the conditions outlined above.

*Article 26*

*Dependence*

1. The competent authority shall verify that an institution supports the assumptions on dependence to the greatest extent possible by an appropriate combination of empirical data analysis and expert judgment.

2. For purposes of Article 26(1), losses within each operational risk category shall be independent of each other. If this is not the case, dependent losses shall be aggregated together and, only if that is not possible, dependence within the operational risk categories shall be appropriately modelled.

3. The competent authority shall verify that an institution carefully considers dependence between tail events. The dependence structure shall not be based on Gaussian or Normal-like distributions.

**Explanatory Box**

The use of a Gaussian or Normal-like copula generally does not appear well suited for operational risk measurements as there is only limited, if any, low-tail dependence. This has the consequence that even Gaussian copulas with high level of correlations or other co-dependencies will not exhibit correlated behaviour at high percentiles. In other words, regardless of how high a correlation is considered, if we go far enough in the tail, extreme events appear to occur independently.

The 2008-2009 crisis indeed made it clear that the use of Gaussian or Normal-like functions and copulas have significantly underestimated market risk and credit risk tail events. As tail events are usually the main drivers of operational risk, which is perceived as more fat-tail kind of risk, dependencies in operational risk and consequently the embedded correlation structures in copulas have to be treated in a more conservative way.

Therefore it is proposed in this consultation paper that Gaussian or Normal-like copulas are not to be used for operational risk modelling. For instance a T-Student copula with few degrees of freedom (e.g. 3 or 4) in most cases appears more appropriate to capture the dependencies between operational risk events.

4. All assumptions regarding dependence shall be conservative given the uncertainties relating to dependence modelling for operational risk. The degree of conservatism shall increase as the rigor of the dependence model and the reliability of the resulting capital requirements estimates decrease.

5. The competent authority shall verify that an institution properly justifies the dependence assumptions and regularly performs sensitivity analyses to assess the effect of the dependence assumptions on its AMA regulatory capital.

## Section IV - Insurance and other risk transfer mechanisms

*Article 27*

*General standards*

The competent authority shall verify that an institution applies the criteria set out in Articles 28 and 29 of this Regulation for the recognition of the insurance and other risk transfer mechanisms ('ORTM') within the AMA regulatory capital.

*Article 28*

*Use of insurance and other risk transfer mechanisms*

1. The competent authority shall verify that an institution uses insurance and ORTM for sound risk management purposes and not only to replace capital. In this regard, the use of insurance and ORTM shall be kept under review and the AMA regulatory capital shall be recalculated, if appropriate, in the event that the nature of the insurance or the coverage of ORTM changes significantly or if there is a major change in the institution's operational risk profile. If a material loss is incurred which affects the insurance coverage, or if changes in insurance or ORTM contracts create major uncertainty as to their coverage, the AMA capital shall be recalculated with an additional margin of conservatism, for example by applying further haircuts in the insurance modelling.

2. The competent authority shall verify that due to insurance or ORTM coverage uncertainties, an institution is always prepared to increase its AMA capital to a gross-of-insurance mitigation or gross of ORTM level, should its insurance or ORTM cover be unexpectedly terminated or reduced for any reason. The competent authority shall verify that an institution calculates capital on a gross- and net-of-insurance and ORTM basis for each capital calculation, at a level of granularity such that the termination of any risk mitigant could be immediately recognised for its effect on capital.

*Article 29*

*Insurance risk mapping process*

1. As part of any application to recognize the risk mitigating impact of insurance, the competent authority shall verify that an institution provides a well-documented and well-reasoned assessment of the way that the insurance coverage is aligned to the institution's operational risk profile.

2. In order to develop an insurance coverage consistent with the likelihood and impact of the losses that an institution may potentially face, the competent authority shall verify that an institution develops and implements an appropriate 'insurance risk mapping process'. The insurance risk mapping process shall fulfil the following conditions:

    (a) it shall map the insurance policies to the institution's own loss categories at the maximum level of detail, by using all the information sources available, including (internal and external) loss data and scenario estimates;

    (b) it shall employ the appropriate expertise and shall be conducted with transparency and integrity;

    (c) it shall assign the appropriate weight to the past and expected performance of insurance through a thorough assessment of the components of the insurance policy;

    (d) it shall obtain formal approval from the appropriate risk body or committee;

    (e) it shall be periodically re-examined.

For the purposes of this provision, 'insurance risk mapping process' means a process where an institution - for all pertinent losses - generates an estimate of the probability of insurance recovery and the possible timeframe for receipt of payments by insurers (such as the likelihood of a claim being litigated, the length of that process and current settlement rates and terms) which is based on the experience of its insurance risk management team, if necessary supported by appropriate external expertise such as claims counsel, brokers and carriers. This process is employed to assess the performance of insurance in the event

of an operational risk loss and can be designed to assess the insurance response for all relevant loss and/or scenario data being entered into the capital model.

*Article 30*

*Insurance modelling and haircuts*

1. In order to be recognized for insurance capital offsetting, the competent authority shall verify that an institution uses a sophisticated modelling approach that is consistent with the AMA methodology adopted to quantify the gross-of-insurance losses and is transparent in its relationship to, and consistent with, the actual likelihood and impact of losses used in the institution's overall determination of its operational risk capital.

2. The competent authority shall verify that an institution investigates the various factors that create payment uncertainty in the effectiveness of the risk transfer, how they have affected the mitigating impact of insurance on the operational risk profile in the past and how they may affect it in the future. The competent authority shall verify that an institution reflects these uncertainties in its capital calculations through appropriate haircuts. The appropriateness of the haircuts shall be calculated conservatively.

3. The competent authority shall verify that an institution explicitly quantifies and models separately the haircuts in relation to the identified relevant uncertainties and does not apply one single haircut covering all uncertainties. This is necessary to provide transparency of assumptions and to appropriately model the responsiveness of the cover.

4. The competent authority shall verify that an institution takes into account the recognition of the insurer claims paying ability risk to the maximum extent, by applying appropriate haircuts in the insurance modelling methodology. This shall provide a more risk sensitive estimate of the impact of insurance and shall allow for the recognition of insurers with different claims paying ability rating above the minimum envisaged by Article 323(2) of Regulation (EU) No 575/2013.

5. The competent authority shall verify that an institution ensures that the claim paying ability risk for counterparty default is assessed on the basis of the credit quality of the

insurance company responsible under the given contract, even if its parent institution has a better rating or the risk is transferred to a third party.

6. The competent authority shall verify that an institution makes conservative assumptions relating to renewal of insurance policies on equivalent terms, conditions, and coverage, as some risks covered by the policy may not be included when the policy is renewed or insurers could decide to cancel policies before contractual expiration.

7. The competent authority shall verify that an institution considers additional characteristics including whether the policies are claims-made or claims-incurred or whether the losses are direct losses or liability losses. The competent authority shall verify that the institution considers and fully document data on insurance pay-outs by loss type in its loss databases and sets haircuts accordingly.

8. The competent authority shall verify that an institution has processes in place to ensure that the exhaustion of policy limits and the price and availability of reinstatements of cover as well the coverage mismatches of medium to large losses due to high deductibles and limits are appropriately reflected in its AMA insurance methodology.

9. For the purposes of this provision, the following definitions shall apply:

   (a) 'coverage mismatch' means the occurrence that the coverage of the insurance contract does not match the operational risk profile of the institution, such that the cover does not provide the "pursued" mitigating effect and some events are not covered;

   (b) 'claims-incurred' means that losses that are incurred during the policy period are covered, even if they are not discovered and the claim is not lodged until after expiration of the policy;

   (c) 'claims made' means that only losses that are claimed or notified to the insurer during the policy term are covered, therefore any loss that is discovered after the policy expires will not be covered by that policy;

(d) 'payment uncertainty' means a risk that the insurance provider will not make the payments expected by the institutions in a timely fashion. The factors that add to the uncertainty of payment of insurance, include but are not limited to:

(i) the willingness of the insurer to pay in a timely manner;
(ii) the ability of the insurer to pay in a timely manner;
(iii) the ability of the institution to identify, analyse and report the claim in a timely manner;
(iv) disputes over the underlying cause of the loss, the fulfilment of necessary precautions (such as the duty to disclose expectations), disputes over the date of occurrence, the amount of the loss, and whether the loss counts as one or multiple events; and
(v) unknown mismatches in cover.

*Article 31*

*Supervisory assessment of insurance mitigation*

1. The competent authority shall assess the use by an institution of the insurance mitigation to offset the AMA regulatory capital, taking into account (i) the relevant insurance policies and (ii) the methodology used by the institution for incorporating the risk mitigation into its measurement model.

2. The competent authority shall recognize the risk-mitigating effect of insurance contracts provided by an undertaking authorized in a third country, if that undertaking satisfies prudential requirements that are equivalent to those applied in the EU and meet the standards set forth in Article 323 of Regulation (EU) No 575/2013.

3. When assessing if the insurance coverage for AMA regulatory capital purposes is provided by a third-party entity, the competent authority shall have a comprehensive view of an institution's consolidated situation as defined by Article 4(1), point (47) of Regulation (EU) No 575/2013 so as to be able to assess that the operational risk has in fact been transferred to an entity in which neither the institution nor any other consolidated entity has a relevant interest.

4. In particular the competent authority shall verify that an institution has taken reasonable steps to ensure that neither it nor any of its consolidated subsidiaries is knowingly re-insuring contracts that cover operational risk events that were the object of the initial insurance arrangement entered into by the institution. If captive or fronting arrangements are used, only that portion where ultimate liability rests with an eligible third-party entity (so that the risk can be seen as being effectively transferred outside of the consolidated entities) shall be considered in the AMA capital calculation.

   For purposes of Article 31(3) and (4), 'third-party entity' means an entity outside the consolidated situation of the institutions seeking insurance protection.

5. The competent authority shall assess the haircuts applied in the AMA insurance modelling carefully, balancing the flexible approach provided by Regulation (EU) No 575/2013 against the need to ensure that the general intent of the rules is not circumvented. For this purpose, the calculation of the haircuts by simple ex-post adjustments shall not be accepted as it may fail to capture the relevant uncertainties of the insurance coverage.

6. The competent authority shall assess that the haircuts for residual and cancellation terms are appropriate in light of the specific characteristics of the institutions insurance policies, including automatic renewal clauses, forward contracts, and/or regular changes to insurance providers.

7. The competent authority may decide to waive an institution from applying haircuts for residual and/or cancellation terms if it can be reasonably assumed that the cover will be renewed and continuous. The following criteria shall be applied:

   (a) haircuts for residual terms may be waived if an institution has in place a replacement contract that provides insurance cover on equivalent terms and without coverage gaps or if the current insurance contract has an automatic renewal provision and no cancellation is possible during the term or at the renewal date;

   (b) haircuts for cancellation terms may be waived if an institution has in place a policy with a cancellation period of more than one year.

8. The competent authority shall assess an institution's procedures for loss identification, analysis and claims processing, as these will have a bearing on the actual coverage protection provided by the insurer or on the ability to receive the claim payment funds within a reasonable timeframe.

9. The competent authority shall assess how an institution (i) has differentiated between first-party direct and third-party liability losses and (ii) has considered the underlying claims basis for each of its policies, in order to determine if these aspects have been treated appropriately in the insurance modelling.

   For purposes of this provision, 'residual term' means the contractual period remaining at a given point in time.

*Article 32*

*Supervisory assessment of other risk transfer mechanisms*

1. The competent authority shall verify that an institution has experience in using ORTM instruments and their characteristics, such as probability of coverage and timeliness of payment, before these instruments can be recognized in the institution's operational risk measurement system. The competent authorities shall also verify that outsourced activities are not considered part of ORTM.

2. As ORTM protection reduces the operational risk exposure of the protection buyer, but it increases the risk exposure of the protection seller, the competent authority shall be aware of the risks assumed by sellers of ORTM protection and shall consider prudential measures if a protection seller acquires significant risk exposures from other institutions. The competent authority shall monitor the use of such products closely and shall assess the intent of the institution in purchasing such instruments when evaluating their risk mitigating effect.

3. The competent authority shall assess an institution's use of ORTM in AMA capital calculations on a case by case basis, considering the eligibility of the protection seller (regulated or unregulated entity) and the nature and characteristics of the protection provided (funded protection, securitization, guarantee mechanism or derivatives).

4. The competent authority shall not accept ORTM as risk mitigation under an AMA if they are held or used for trading purposes rather than for risk management.

5. The competent authority shall be mindful that stricter qualifying criteria may be required for the eligibility of ORTM providers and the type of ORTM products for the following reasons:

    (a) the peculiarities of operational risk relative to credit risk, such as the absence of underlying assets and the greater role of unexpected losses;

    (b) the lack of an efficient, liquid, and structured market for analogous products which thus far have been traded outside the banking sector, such as catastrophe bonds and weather derivatives; and

    (c) the difficulty in assessing the legal risk of ORTM, even when the terms and conditions of the contracts are clearly and carefully spelt out.

## Section V – Capital Allocation

*Article 33*

*Allocation mechanism*

1. The competent authority shall verify that an institution's capital allocation mechanism is consistent with the institution's risk profile and is on forms with the overall design of the operational risk measurement system For this purpose, the competent authority shall verify the following:

    (a) In the case of an institution operating on a consolidated basis, the competent authority shall be satisfied by the level of integrated management, risk management and internal control related to operational risk regarding the entities that would be included in the scope of prudential consolidation;

(b) Capital allocation shall take into account potential internal differences in inherent risk and quality of operational risk management and internal control between the business lines/units to which capital is allocated.

(c) No current or foreseen practical or legal impediment to the prompt transfer of own funds or repayment of liabilities shall be observed;

(d) Capital allocation from the consolidated group level downwards to subsidiaries and/or business lines involved in the consolidated AMA calculation process shall rely on sound and rational methodologies implemented consistently, fairly, and with integrity.

## Section VI – Parallel Running

*Article 34*

*General principles*

1. The competent authority shall verify that an institution that intends to apply for permission to use AMA parallel runs its old and new systems for calculating the operational risk own funds requirement for a period which is sufficient for the competent authority to establish that the institution meets the qualitative and quantitative standards set out in Articles 321 and 322 of Regulation (EU) No 575/2013 and the general risk management standards set out in Articles 74(1), 76(2), 76(3), 76(4) and 85(1) of Directive 2013/36/EU.

2. In order to demonstrate the stability and robustness of the AMA output and to benchmark the AMA capital figure against the former approach, the competent authority in granting the permission to use the AMA shall request the institution to continue to parallel run for one year after the permission is granted.

*Article 35*

*Parallel running outputs*

1. The competent authority shall verify that, during the period of parallel running, an institution calculates, on at least a quarterly basis, its operational risk regulatory capital requirement according to the old and to the new basis.

2. Pending the competent authority's assessment of AMA application, an institution shall calculate and submit to the competent authority - at least three months before the competent authority makes its decision - the most recent (minimum of 2 quarters) Pillar 1 operational risk regulatory capital requirement calculated using both operational risk measurement system and the existing methodology for:

    (a) all relevant legal entities and/or operational risks that will use an AMA at the date of the initial implementation;

    (b) the institution on a consolidated basis.

**Explanatory Box**

Parallel running is the simultaneous operation by an institution of its existing system and new system (AMA) to measure the institutions operational risk own funds requirement. Parallel running is roughly comparable to a systems evaluation exercise performed by institutions when introducing new software.

Parallel running is an integral part of the supervisory assessment process because it helps provide an insight of the extent to which the bank's internal operational risk measurement system will be closely integrated into its day-to-day risk management processes.

The assessment process should consider a minimum of two quarterly capital estimations data points, submitted at least three months before the competent authority makes a decision whether to grant or refuse permission for the firm to use AMA.

*Article 36*

*Parallel running criteria*

1. The competent authority shall assess how parallel running has enabled the institution to:

(a) develop and test the risk management framework and capital calculation system;

(b) resolve problems and fine-tune the system and attendant processes;

(c) ensure that the capital calculation system generates results which conform to the institution's prior expectation, including taking account of information from their existing / legacy systems;

(d) quickly vary model parameters to understand the impact of changed assumptions with minimal systems adjustments or manual interventions;

(e) make appropriate capital adjustments to the regulatory capital before the first date of 'live use';

(f) demonstrate that the new systems and reporting processes are robust over a reasonable period and generate management information that the institution can use to identify and manage operational risk.

## CHAPTER V

## DATA QUALITY AND IT INFRASTRUCTURE

*Article 37*

*General principles*

1. The competent authority shall verify that data flows and processes associated with operational risk management and measurement are made transparent and accessible by an institution.

2. The competent authority shall verify that the quality of data used in the AMA is maintained over time and for this purpose that the building and maintenance procedures are regularly analysed by the institution.

> **Explanatory Box**
>
> Accessibility could be limited e.g. in case of outsourced processes or done by other units of the institution. Accessibility means accessible for the authorized staff of an institution and accessible for the competent authority supervisors (see also CRR, Art 321g).
>
> Building procedures means a "System Development Life Cycle", SDLC.

3. The competent authority shall verify that an institution ensures:

    a. the quality of data on a continuing basis;

    b. the soundness, robustness and performance of the IT infrastructure used for AMA purposes.

4. The use of external data sources or the outsourcing of some parts of the IT infrastructure management does not exempt an institution from complying with these standards.

*Article 38*

*Data quality*

1. For purposes of Article 37(3), lett. (a), an institution shall have at its disposal the following sets of due quality data:

    a. Data to build and track its operational risk history (internal and external data, scenarios and BE&ICF);

    b. Other complementary data, such as model parameters, model outputs and reports.

*Article 39*

*Supervisory assessment of data quality*

1. The competent authority shall verify that the information included in the institution's archives is compliant with the Articles 321 and 322 of Regulation (EU) No 575/2013.

2. The competent authority shall verify that an institution has defined appropriate data quality dimensions to provide effective support to its operational risk measurement and management processes. Moreover the competent authority shall verify that an institution complies on regular basis with the set dimensions.

**Explanatory Box**

Core dimensions of data quality are very often indicated as: Completeness, Relevance, Timeliness, Validity, Accuracy, and Consistency. Indeed there are many others dimensions and the practice of data quality suggests defining which dimensions are of interest with respect the business scope. Understanding the key data quality dimensions is the first step to data quality assessment.

Completeness is defined as the extent to which data are of sufficient breadth, depth, and scope for the task at hand. A null value in a data set is an example of incomplete data.

Relevance is the degree to which data meet current and potential user needs. It refers to whether all data that are needed are produced and the extent to which concepts (definitions, classifications etc.) reflect user needs.

Timeliness, concerns how promptly data are updated. It reflects the length of time between its availability and the event or phenomenon it describes.

Validity is a measure that indicates whether the data make sense in the scope of their usage.

Accuracy is defined as the closeness between a value v and a value v', considered as the correct representation of the real-life phenomenon that v aims to represent.

Consistency is the absence of any violation of a business rule in a database. In the relational model of data, any violation of referential integrity is an example of inconsistency. This consistency must be maintained over time statically and dynamically and significant discrepancies discovered in regular consistency checks, that include audit trails of data sources, should be investigated.

3. The competent authority shall verify the appropriateness of the documentation for the design and maintenance of the databases used in the AMA framework.

4. For the purposes of Article 39(3), the competent authority shall verify that the documentation contains at least:

    (a) global map and descriptions of databases involved in the operational risk measurement system;

    (b) data policy and statement of responsibility;

    (c) work-flows and procedures related to data collection and data storage;

(d) statement of weaknesses with the all weaknesses found in the databases validation and review processes and a statement how the institutions plans to correct or reduce the weaknesses.

5. The competent authority shall verify that SDLC policies for AMA system are approved by the institution's management body and senior management.

*Article 40*

*Supervisory assessment of IT infrastructure*

1. The competent authority shall verify that the IT systems and infrastructure for AMA purposes are sound and resilient and that these features can be maintained on a continuous basis.

**Explanatory Box**

Soundness refers to the capacity of the infrastructure to support the ordinary and extraordinary processes on a continuous, automatic and flexible basis avoiding IT risks while providing correct data processing

Resiliency is the ability of a server, network, storage system, or an entire data center, to recover quickly and continue operating even when there has been an equipment failure, power outage or other disruption.

2. The competent authority shall verify that information security, IT risk management and IT processes for AMA purposes are based on appropriate standards and that the controls and measures are effective.

**Explanatory Box**

Such appropriate standards could be ISO 270xx family- information security management, IT risk management and ISO 20000 - IT Service management.

3. The competent authority shall verify that the SDLC for AMA purposes satisfies the best practice for software systems, which ensure sound and proper:

(a) project management, risk management, and governance;

(b) requirements engineering, quality assurance and test planning;

(c) systems modelling;

(d) systems development;

(e) quality assurance in all activities (including code reviews and if appropriate, code verification), and

(f) testing, which includes user acceptance.

4. The competent authority shall verify that an institution's IT infrastructure implemented for AMA purposes are subject to configuration management, change management and release management processes.

5. The competent authority shall verify that effective controls for outsourcing or sourcing of any component of the AMA system are in place.

6. The competent authority shall verify that SDLC and contingency plans for AMA purposes are approved by an institution's management body or senior management and that the management body and senior management are periodically informed on the IT infrastructure performance for AMA purposes.

## CHAPTER VI

## USE TEST

*Article 41*

*Use test (not limited to regulatory purposes)*

The competent authority shall verify that an institution ensures that the purpose and use of AMA are not limited to regulatory purposes, rather that:

(a) an institution operational risk measurement system is integrated in its day-to-day business process and used for risk management purposes on an on-going basis;

(b) the operational risk measurement system is used to manage operational risks across different business lines/units or legal entities within the organisation structure;

(c) the operational risk measurement system is embedded within the various entities of the group. In case of use of an AMA at consolidated level, the parent's AMA framework has to be rolled out to the subsidiaries, and the subsidiaries' operational risk and controls have to be incorporated in the group-wide AMA calculations.

(d) the operational risk measurement system is not only used for the calculation of the institution’s regulatory own funds requirement in accordance with Articles 92(2)(e) and 312(2) of Regulation (EU) No 575/2013, but also for the purposes of its internal capital adequacy assessment process in accordance with Article 73 of Directive 2013/36/EU.

**Explanatory Box**

For an institution adopting the internal model for calculating the operational risk regulatory capital, the AMA is the reference model for both Regulatory and Internal capital calculation. The outputs of the two models should not be materially different and should be easily and readily explainable.

*Article 42*

*Evolving nature*

The competent authority shall verify that an institution ensures that the AMA evolves as the institution gains experience with risk management techniques and solutions, by assessing that:

(a) an institution's operational risk measurement system is robust and responsive to the institution's changing dynamic;

(b) the operational risk measurement system is updated on a regular basis and evolves as more experience and sophistication in management and quantification of operational risk is gained;

(c) the nature and balance of inputs into the operational risk measurement system are relevant and continuously fully reflect the evolving nature of an institution business, strategy and operational risk exposure.

*Article 43*

*Supporting and enhancing operational risk management*

The competent authority shall verify that an institution ensures that the AMA supports and enhances the management of operational risk within the organization, by assessing that:

(a) inputs and outputs of an institution's operational risk measurement system contribute to and are used in their management and decision-making processes;

(b) the operational risk measurement system contributes to the regular and prompt reporting of appropriate and consistent information that fully reflects the nature of the business and its risk profile;

(c) remedial action for improving processes is considered upon receipt of information from the operational risk measurement system.

*Article 44*

*Beneficial for operational risk organization and control*

The competent authority shall verify that an institution ensures that the use of AMA provides benefits to the institution in the organization and control of operational risk, by assessing that:

(a) the institution's definition of operational risk appetite and tolerance and its associated operational risk management objectives and activities are clearly communicated within the organisation;

(b) the relationship between the institution's business strategy and its operational risk management (including with regard to the approval of new products, systems and processes) are clearly communicated within the organisation;

(c) there is evidence that the operational risk measurement system increases transparency, risk awareness and operational-risk management expertise and creates incentives to improve the management of operational risk throughout the organisation;

(d) inputs and outputs of the operational risk measurement system are used in relevant decisions and plans, such as in the institution's action plans, business continuity plans, internal audit working plans, capital assignment decisions, insurance plans and budgeting decisions.

## CHAPTER VII

## AUDIT AND INTERNAL VALIDATION

*Article 45*

*Audit and internal validation reviews*

1. The competent authority shall verify that an institution's audit and internal validation functions verify on regular basis whether the operational risk management and measurement processes implemented for AMA purposes are reliable and effective in managing and measuring operational risk within the organization.

2. In particular, the competent authority shall verify that, at least on annual basis:

    (a) the internal validation function provides a reasoned and well-informed opinion on whether the operational risk measurement system works as predicted, and whether the outcome of the model is suitable for its various internal and supervisory purposes;

    (b) the audit function verifies the integrity of the operational risk policies, processes and procedures, assessing whether these comply with legal and regulatory requirements as well with established controls. For this purpose, emphasis shall be provided to the verification of the quality of the sources and data used for operational risk management and measurement purposes.

3. The competent authority shall verify that these functions have a review program in place that cover the aspects of the AMA included in Chapter I to VI of this Regulation and is regularly updated with regard to:

    (a) the development of internal processes for identifying, measuring and assessing, monitoring, controlling and mitigating operational risk; and

    (b) the implementation of new products, processes and systems which expose the institution to material operational risk.

4. The competent authority shall verify that the internal validation is carried out by an institution's qualified resources, which are not dependent of the validated units.

5. The competent authority shall verify that, where audit activities are carried out by internal or external audit functions or qualified external parties, these are independent of the process or system being reviewed. In case of outsourcing of the internal audit activity, the management body and senior management are accountable for ensuring that outsourced functions are performed in accordance with the institutions' approved audit plan.

6. The competent authority shall verify that the audit and internal validation reviews on the AMA framework are properly documented and their output distributed to the appropriate recipients within the institutions, such as the risk committees, operational risk management function, business line management and pertinent staff, if appropriate.

7. The competent authority shall verify that results of the audit and internal validation reviews including senior management's attestation are summarized and reported at least annually to the institutions management body, or a committee thereof, for approval. Attestation by senior management entails review and approval of the effectiveness of the institution's AMA framework on an annual basis.

*Article 46*

*Assessment of audit and internal validation*

1. The competent authority shall assess, as part of its activities, audit programs for reviewing the operational risk framework that cover all significant activities – including outsourced activities – exposing an institution to material operational risk.

2. The competent authority shall assess the internal validation function according to the following principles:

    (a) clarity and appropriateness of the methodology for the organisation and for its AMA framework, and clear documentation;

    (b) proportionality of the internal validation techniques and their consideration of changing market and operating conditions;

(c) comprehensiveness of the internal validation, encompassing both quantitative and qualitative elements;

(d) effectiveness of the internal validation processes and outcomes that shall be subject to audit review.

3. The competent authority shall verify that the audit and internal validation functions and their reviews comply with the following elements:

(a) independence;

(b) capacity;

(c) professional competence; and

(d) critical analysis.

**Explanatory Box**

Independence - the bank's audit and internal validation functions shall provide independent assessments and opinions, while avoiding improper influence from those units being reviewed. Personnel conducting reviews shall not be involved in the development, implementation or operation of the Operational risk processes or systems being reviewed, or be subordinate to the units under review.

Capacity - audit and internal validation functions shall be adequately staffed and have reasonable access of resources to perform their duties. The board and senior management are responsible for ensuring that these functions are appropriately staffed.

Professional competence - bank staff performing audit and validation work shall be technically competent, appropriately trained and possess the appropriate skills.

Critical Analysis - audit and internal validation functions shall critically analyse all relevant information by questioning the work of the units involved in the design of the operational risk management processes and measurement systems.

## CHAPTER VIII

## FINAL PROVISIONS

*Article 47*

*Entry into force*

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

For the institutions already using an AMA for regulatory purposes, this Regulation shall apply after one year from its entry into force.

Article 6(1) shall apply after two years from the entry into force of this Regulation. Article 6(3) shall apply after one year from the entry into force of this Regulation.

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

Done at Brussels,

*For the Commission*
*The President*

*[For the Commission*
*On behalf of the President*

*[Position]*

# 5. Accompanying documents

## 5.1 Draft impact assessment

### Introduction

Article 312(4) of Regulation (EU) No 575/2013 requires the EBA to develop draft Regulatory Technical Standards (RTS) related to the assessment methodologies for Advanced Measurement Approaches (AMA).

Article 10(1) of the EBA Regulation (Regulation (EU) No 1093/2010 of the European Parliament and of the Council) provides that when any draft implementing technical standards/regulatory technical standards developed by the EBA are submitted to the EU Commission for adoption, they should be accompanied by an analysis of 'the potential related costs and benefits'. This analysis should provide the reader with an overview of the findings regarding the problem identification, solutions proposed and the potential impact of these options.

This annex presents the impact assessment with a cost-benefit analysis of the provisions included in the RTS described in this Consultation Paper. Given the nature of the study, the impact assessment is high level and qualitative in nature.

### Procedural issues and consultation process

The EBA prepared a questionnaire addressed to national competent authorities (NCAs) to obtain information on current practices in the EU Member States and expected costs and benefits related to the adoption of the RTS on assessment methodologies for AMA. This analysis is based on the responses to the questionnaire.

The draft RTS are largely based on the current CEBS Guidelines 'Guidelines on the Implementation, Validation and Assessment of Advanced Measurement Approaches (AMA) and Internal Ratings Based (IRB) Approaches' (GL-10 CEBS, 'CEBS GLs'). The questionnaire mapped each article of the draft RTS into the corresponding section of the CEBS GLs and asked about the current level of implementation (i.e. the baseline) and expected costs and benefits for all the chapters of the draft RTS, with the exception of Chapter I (which deals with definitional aspects), as follows:

- Scope of operational risk and operational loss;
- Operational risk management;
- Operational risk measurement;
- Data quality and IT system;

- Use test; and
- Audit and validation.

The respondents were asked to indicate separately the level of implementation and the expected costs and benefits from zero (no implementation/cost/benefit) to three (full implementation/high cost/benefit). For the sake of simplicity, the scope of the questionnaire was restricted to home institutions only.

At the time of drafting, the EBA has received seventeen responses from NCAs,

of which eight confirmed that there are no institutions using AMA under their home Member State supervision.

### Problem definition

This section outlines the problems to be addressed by these RTS. The core problem that the RTS aim to address is the lack of harmonisation in current practices for the assessment methodology under which the competent authorities permit institutions to use AMA.

Due to the non-binding nature of the CEBS GLs, both the interpretation and the implementation of the assessment methodology, conditions and the modalities vary across EU Member States. For example, the risk profile of an institution depends on the scope of the operational risk and the operational loss, and the scope depends on the assessment methodology under which the competent authorities permit institutions to use AMA models. If the interpretation and the implementation of the assessment methodology are not consistent across EU Member States, the framework may lead to regulatory problems in the EU banking sector, including:

- An uneven level playing field: if the conditions and parameters for assessment are not consistent between jurisdictions, two institutions located in two different jurisdictions may be treated differently, although despite having the same operational risk profile;
- Regulatory arbitrage: institutions cease their operations in a Member State where the regulatory framework is stricter and/or less predictable and relocate their businesses to Member States with a more favourable regulatory framework.

On a larger scale, such problems in the regulatory framework may prevent the effective and efficient functioning of the EU banking sector as well as the internal market.

Another problem related to the AMA models is the effectiveness of the current framework in responding to new challenges in the EU banking sector. The current framework is based primarily on the CEBS GLs and it is reasonable to consider that the current RTS, of which CEBS GLs are the basis, will provide an updated version of these and establish a regulatory framework that addresses the challenges in the banking sector. The logic behind the Section (0) of technical

options is based on this argument. Section (0) of the assessment of technical options presents a qualitative analysis and identifies an optimal option that can effectively address the problems identified.

### Baseline scenario

There are significant variations between EU member states in the number of AMA institutions and their asset shares.

It is therefore reasonable to expect that the impact of these RTS will also vary between States. Since the CEBS GLs form the basis of the RTS, compliance with the former can be assessed as a benchmark in order to identify the current level of implementation of the RTS, i.e. looking at the level of compliance with the CEBS GLs to understand where each EU Member State currently stands in terms of meeting the content of the RTS.

It is reasonable to assume a negative correlation between the level of compliance and the expected costs and benefits that the RTS will generate in the future. For example, if a Member State is currently in full compliance with the CEBS GLs then the costs and benefits are predicted to be low or negligible after the implementation of the RTS.

In the sample, all Member States are either in full compliance or mostly comply with the CEBS GLs.

### Objectives of the technical standards

The main specific objectives of the technical standards are to:

- update the regulatory framework related to operational risk to respond effectively to the challenges of the current banking system; and
- harmonise the standards for the supervisory framework on AMA models to minimise room for regulatory arbitrage and distortions in the EU banking sector.

### Technical options

In line with the problem definition, the following possible approaches to the development of the technical standards were considered:

**Option 1:** converting the CEBS GLs fully into RTS with no additional elements;

**Option 2:** converting CEBS GLs into RTS with additional elements;

**Option 3:** converting CEBS GLs partially into RTS with no additional elements.

The logic behind the technical options is to capture the extent to which the current framework under CEBS GLs addresses the challenges of the banking sector in relation to operational risk. In other words, it discusses qualitatively whether:

- the current framework is sufficient to completely and effectively meet the objectives (Option 1);
- the current framework is not sufficient and new elements therefore need to be added (Option 2); or
- the current framework includes outdated elements that are no longer relevant to the current banking sector and can therefore be excluded to allow the current framework to effectively meet the objectives (Option 3).

### Assessment of the technical options

The assessment of the options is based on the responses to the questionnaire, in which NCAs were asked to indicate the level of expected costs and benefits and to provide the sources of these costs and benefits.

### Option 1

Under this option, the content of the RTS is identical to that of the CEBS GLs. The basis of the latter is the supervisory experience and expectations for the implementation, validation and assessment of AMA models as of the beginning of 2006. CEBS GLs are no longer effective at addressing the new challenges in the EU banking sector, particularly those related to the collection and handling of internal loss data, and operational risk modelling and insurance.

In their responses to the questionnaire, all NCAs attributed negligible cost to the relevant sections of the RTS. This is due to the already high level of compliance with the CEBS GLs and the unavailability of the AMA institutions in the relevant jurisdiction.

In terms of the benefits of the option, NCAs with AMA home institutions under their supervision considered the benefits from the identical transformation of the CEBS GLs into RTS for all chapters in the legislation to be negligible or small. Two NCAs considered the benefits to be negligible and small depending on the chapters of the RTS, while only one Member State predicted significant benefits from this option. The major source of the benefits is the level of harmonisation across Member States and the certainty that all provisions of the previous Guidelines, which were not legally binding, would be implemented in a comprehensive and consistent manner.

In addition, Member States with no AMA institutions under their home supervisory jurisdiction can also benefit from the policy, since a more effective regulatory framework will generate positive externalities. This is particularly true given that the EU banking sector is highly interrelated and operates with a high level of cross-border elements.

### Option 2

Option 2 is an extended version of Option 1, incorporating additional elements into the CEBS GLs before transforming them into the RTS. The RTS containing the additional elements are expected to address the problems relating to operational risk more effectively. These additional elements mainly cover the collection and handling of internal loss data, operational risk modelling and insurance. Under this option, the RTS incorporates CEBS GLs with The Basel Committee on Banking Supervision (BCBS) AMA Supervisory GLs and the BCBS Insurance Paper in the areas of:

- Gross loss definition;
- Date of internal loss;
- Granularity;
- Distributional assumptions;
- Dependence;
- Use of the four elements([7]);
- Criteria for recognising insurance mitigation;
- Insurance modelling;
- Haircuts, discounts and uncertainty.

In terms of the impact of this option, the magnitude of the associated costs and benefits depends on the technical area of the RTS. The remainder of the section assesses this option for each chapter of the RTS. The following general conclusions can be drawn from the analysis:

- There is no RTS chapter under which any Member State expects greater costs than benefits;
- For some chapters, Member States indicate that the costs will offset and balance out the benefits, and for one Member State, this is the case for all chapters;

[7] According to Article 322(2)(b) of Regulation (EU) No 575/2013, an AMA Institution must use the following four elements to build its operational risk measurement system: internal loss data, external loss data, scenario analysis and business environment and internal control factors.

- At the EU level, under all chapters, the benefits of the RTS are greater than the costs (i.e. the aggregate net benefit is positive for all chapters); and

- Net benefits are greatest for the chapters on operational measurement, data quality and IT system, and audit and validation.

### a. Costs and benefits related to the scope of operational risk and operational risk loss:

The responses received from the Member States indicate that 60% of the NCAs expect low costs associated with 'the scope of operational risk and operational risk loss' under Option 2 and about 30% of respondents expect negligible costs in the same area. These costs for the NCAs and the industry are expected to be incurred mainly from the implementation of the provisions. The additional data collection process, the one-off cost to establish appropriate IT mechanisms, and operational arrangements to draw the boundary between operational risk and credit risk are stated as the main sources of costs for the industry. Some NCAs stated that additional costs for the national supervisors are expected due to the implementation of new provisions.

In terms of benefits, around 60% of respondents stated that the estimated benefits would be more than small (i.e. medium or large). The provision is expected to clarify the definition and common understanding of operational risk throughout EU Member States, and therefore increase legal certainty and standards in the field of classification and measurement across institutions and Member States, and in terms of operation risk prevention/mitigation in lending activities.

Overall, NCAs believe that the benefits of Option 2 exceed the costs in this particular thematic area.

### b. Costs and benefits related to operational risk management:

Member States indicated that the costs generated under this policy area would be either negligible (about 50% of the NCAs) or low (40% of respondents). Although most of the NCAs did not elaborate on this point, it is reasonable to assume that negligible/low costs are foreseen due to the high level of compliance with the CEBS GLs. Some Member States mentioned low costs that could be incurred due to the amendment of the national regulatory framework and minor adaptations of the AMA models for the existing institutions.

On the other hand, the same NCAs also expect the benefits in this technical area to be negligible. This is reasonable since these Member States are already in extensive/full compliance with the current framework. Some Member States see great benefits in the option in this technical area of the RTS and believe that the benefits significantly exceed the costs. Legal certainty and harmonisation across EU Member States is considered to be the major benefit of the option.

### c. Costs and benefits related to operational risk measurement:

The technical area is the one that incorporates a great number of new elements from other resources before transforming the CEBS GLs into the RTS. Therefore, this is an area in which these RTS will have a great impact. Around 90% of Member States expect low or negligible costs under this option while about 60% think that the benefits will be medium or large. NCAs expect to incur a one-off cost for amending institutions' internal documents. The majority of the NCAs do not expect additional costs in terms of workload since they already apply the relevant provisions under the current framework. They also consider the new elements to be a good addition to the current CEBS GLs in terms of establishing clear definitions and standards.

One Member State indicated that the costs would be incurred from parallel running of the two methods. The current draft includes a proposal requiring the old and the new method to be run in parallel until the institution applies for the new method (Article 34–36). This requirement will introduce some additional costs for institutions, and to a certain extent for the regulators. However, the benefits of being able to evaluate of the effect of the new model also justify this cost.

### d. Costs and benefits related to data quality and IT infrastructure:

The respondents indicated that while the costs associated with this chapter of the RTS are negligible, the expected benefits can vary across Member States. About 40% of respondents expect negligible costs with the RTS requirements under 'Data quality and IT infrastructure'. One Member State argued that the cost would be relatively high due to the additional training required for staff. In this policy area, costs associated with amendments to the national legislation are not expected.

The expected benefits among the Member States vary: while the same 40% of NCAs that indicated negligible costs expect negligible benefits, 60% of the NCAs expect benefits at either a medium or high level. The benefits are mostly associated with the transition from initially more implicit requirements to a clear and detailed assessment of the IT infrastructure.

### e. Costs and benefits related to use test:

Similarly to the previous thematic area, Member States will incur negligible costs due to the RTS requirements on 'use test'. This is indicated by 50% of respondents. Around 40% and 10% of the NCAs think that the costs will be low and medium respectively. No NCA expects a high level of costs associated with the RTS requirements under this thematic area. The NCAs are expected to incur costs from the implementation of new elements in the supervisory approach and no additional costs are expected to fall on the institutions.

The same Member States – 50% of the respondents – that expect negligible costs also see negligible benefits in this thematic area. However, the other half of the Member States in the

sample, which expect low costs, expect to see a greater benefit from the policy intervention. As above, most of the benefits generated from the RTS are due to harmonisation and the establishment of a clearer set of rules that will shape the regulatory framework.

Overall, the benefits are expected to exceed the costs.

### f. Costs and benefits related to audit and validation:

Half of the EU Member States with institutions using AMA models expect negligible costs for NCAs and the industry. The same Member States also stated that the benefits they expect to gain from the intervention are negligible. Around 40% of respondents expect the benefits to exceed the costs. While 30% of respondents indicated low costs and high benefits, one Member State specified low costs and medium-level benefits associated with the RTS requirements under this thematic area. Finally, one Member State indicated that the costs and benefits (that are greater than negligible) will cancel each other out.

Member States that indicated costs would be more than negligible stated that they do not expect any costs for the supervision but they do expect costs for the institutions, especially in relation to the independence of the validation function from the function under review. The institutions will now need to comply with more specific and stringent requirements for their internal audit and validation functions.

The major benefit of the policy is the establishment of harmonised processes throughout the Member States and of a more specific list of tasks and responsibilities of the internal audit and validation functions. On aggregate, the benefits of the policy intervention in this area are expected to exceed the costs.

## Option 3

This option proposes that the RTS cover the CEBS GLs only partially and do not include any new elements. The option is not effective at addressing the problems and new challenges in the field of operational risk because, as argued above, the CEBS GLs that set the current framework need to be complemented and updated before becoming binding in the form of RTS. Therefore, the analysis does not elaborate further on this option.

## Preferred option

Given the formulation of the RTS, Option 2 is the option that will most effectively address the identified problems. Firstly, it updates and fills the gaps in the current regulatory framework, and secondly, the expected net benefits from the implementation of Option 2 are greatest.

## 5.2 Overview of questions for Consultation

Q1: Are the provisions included in these draft RTS on the assessment methodologies for the Advanced Measurement Approaches for operational risk sufficiently clear? Are there aspects that need to be elaborated further?

Q2: Do you support the treatment under an AMA regulatory capital of fraud events in the credit area, as envisaged in Article 6? Do you support the phase-in approach for its implementation as set out in Article 48?

Q3: Do you support the collection of 'opportunity costs/loss revenues' and internal costs at least for managerial purposes, as envisaged in Article 7(2)?

Q4: Do you support the items in the lists of operational risk events in Articles 4, 5 and 6, and the items in the list of operational risk loss in Article 7? Or should more items be included in any of these lists?

Q5. Do you support that the dependence structure between operational risk events cannot be based on Gaussian or Normal-like distributions, as envisaged in Article 26 (3)? If not, how could it be ensured that correlations and dependencies are well-captured?

Q6: Do you support the use of the operational risk measurement system not only for the calculation of the AMA regulatory capital but also for the purposes of internal capital adequacy assessment, as envisaged in Article (42)(d)?