9 January 2026
ESMA42-1710566791-6326

Principles on risk-based supervision

Table of Contents

1 Introduction

1.1 Background

A risk-based approach is a cornerstone of EU securities markets supervision. It is critical for National Competent Authorities (NCAs) and ESMA, thereafter referred to as "supervisory authorities" or "authorities" – to be able to identify, prioritise, mitigate, and manage risks. This is particularly relevant in light of rapid and frequent changes in market conditions, accelerating financial innovation, the increased prominence of cross-border activities and the growing number of interdependencies across markets and their participants.

Effective risk-based supervision (**RBS**) across the EU is key to furthering the single EU market. A risk-based approach to supervision, adopted across various fields of financial supervision, allows for prioritisation on those risks of greatest threat to investor protection, financial stability, and orderly markets. Across the EU, the development of **a consistent, proportionate, and effective** approach is therefore essential.

1.2 Purpose and Scope

The principles in this document aim to promote the development of **a common EU supervisory culture** as provided for in the ESMA regulation[1].

These principles **apply to NCAs and ESMA when carrying out direct supervision**. They are intended to apply to all mandates (markets, entities and products) under an authority's remit and focus on the supervision of those mandates. While different models for risk-based supervision exist, this document introduces an entity-based approach. This can be adapted to other identification models (such as transaction or product based) depending on an authority's supervisory process.

This common framework enables ESMA and NCAs to foster a consistent and effective supervisory approach across sectors, optimising resource deployment. By establishing a shared foundation on risk-based supervision, the principles promote a level playing field and contribute to the ongoing effort toward supervisory convergence.

The **main concepts and processes in this document** concern:

- Definition and understanding of risk-based supervision
- Risk identification
- Risk assessment
- Risk prioritisation and treatment

These principles provide guidance to supervisory authorities when carrying out supervision. They **do not constitute a one-size-fits-all common model** nor a fully-fledged manual on

risk-based supervision. Rather, they are intended to **complement pre-existing frameworks**, providing elements that promote the effective and consistent application of supervisory capabilities, building on collective practices across the EU.

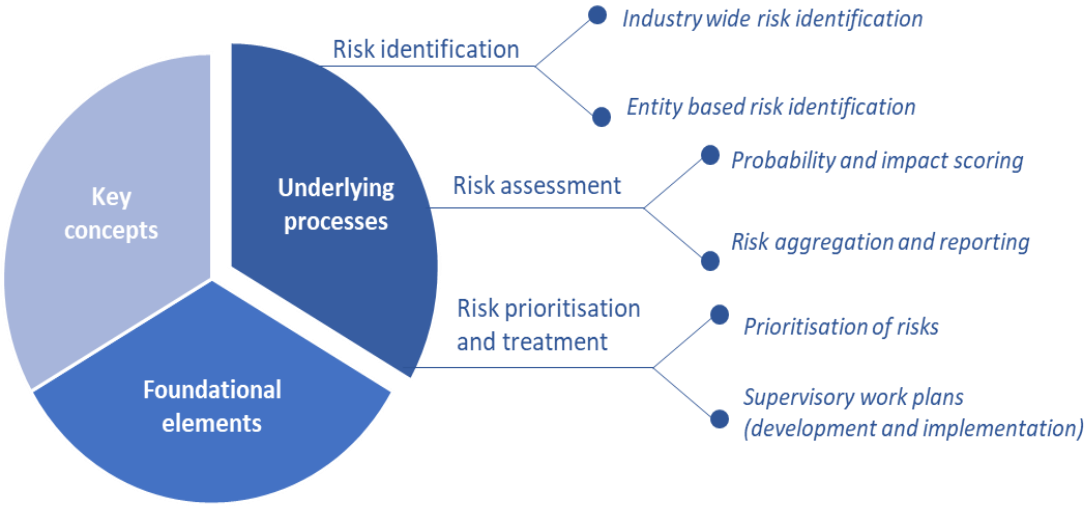
To achieve this objective, these **non-binding** principles are expected to be practically implemented under the relevant authority's framework.

When following the guidance from these principles, NCAs are expected to use their **supervisory judgment**, and to consider the specific risks and characteristics of their national market and the entities (including products offered) under their supervision.

2 Structure of this document

This document is structured using the format outlined in the graphic below.

First, it considers the key concepts of risk-based supervision which describes what it means to be a risk-based supervisor, including some key organisational mind-sets that are needed to ensure its effective implementation. Second, it explains the foundational elements which are the key structures that support the successful implementation of a risk-based approach, notably the supervisory strategy and the risk management framework. Finally, it extrapolates the key processes needed to undertake a risk based supervisory approach.



[1] Article 29(2) - The Authority may, as appropriate, develop new practical instruments and convergence tools to promote common supervisory approaches and practices.

3 Key concepts of risk-based supervision

1. **RBS focuses supervisory attention and resources on the most significant risks**. It promotes a holistic understanding of risks in financial markets and an efficient use of supervisory resources, to ensure authorities achieve their objectives, including protecting investors, financial stability, and orderly markets. It recognises that given the size and complexity of markets, the multitude of entities and activities, and the available supervisory resources, choices need to be made in selecting which risks to address to maximise supervisory effectiveness.

2. **RBS differs from a rule-based approach** which strives to check compliance with the entire regulatory framework regardless of the differences in risks that entities and industry dynamics can pose, and the different supervisory efforts they would require.

3. **RBS does not seek to eliminate all risks.** Rather, it provides a structured and transparent framework to identify, assess, prioritise and treat risks to address them appropriately.

4. **RBS addresses the risks arising from illegal or harmful practices.** Such occurrences could have detrimental outcomes for markets and investors, reduced transparency for supervisors, and increased vulnerability of the financial system.

5. **RBS is flexible as risks vary in size, scope and complexity and change over time, as financial markets are continuously evolving**. This flexibility allows adaptation to emerging risks, such as those posed by changing market structures and technological advancements, including novel or non-traditional ones which may not be sufficiently covered under existing legislation.

6. **RBS recognises that authorities do not operate in isolation, risks are increasingly cross-border and effective international cooperation is necessary**. Considering how risks may manifest beyond national boundaries, understanding entities' global footprint is essential. Timely and proactive engagement, sharing of data and supervisory observations between authorities, and acting concertedly are integral aspects of RBS.

7. **RBS in individual authorities closely interact with EU-wide risk assessments**, given financial markets' increasing interconnectedness and interdependencies. ESMA's risk assessment exercises inform national assessments by providing intelligence on EU-wide supervisory risks. This is achieved through the shared intelligence and extensive expertise of NCAs and ESMA and their collective input to EU wide risk assessment exercises.

8. **RBS recognises that some risks can be entity-specific or industry-wide and be displayed across sectors**. Interaction with other regulatory bodies that have responsibility for such risks (i.e., cybersecurity, macro-prudential, energy, competition) can further help in addressing them.

9. **RBS is based on the use of a common framework to facilitate comparability and consistency across authorities' mandates**. While recognising the heterogeneous remit of

authorities' mandates, and the need to tailor approaches for different sectors (including participants and products) of financial markets, RBS is built on a consistent framework centered on the identification, assessment, and prioritisation of risks.

10. **RBS is forward looking**. It aims to identify and manage risks to the greatest extent possible before they materialise.

11. **RBS is a continuous and recurrent process.** It evolves and iterates over time. It includes a recurring process with a clear feedback loop where authorities test the adequacy and accurateness of risk identification, assessment and prioritisation and adjust where room for improvement is identified.

12. **RBS enables the concept of proportionality**, whereby the supervision level and intensity is commensurate to the level of risk identified. This considers the nature, scale and complexity of the entity, product or activity and their potential effects on investor protection, financial stability, and orderly markets.

13. **RBS facilitates taking a holistic view and prioritising across mandatory activities, inherent and emerging risks**. Authorities face: (i) mandatory activities, to conduct regardless of the level of risk involved; (ii) inherent or recurring risks on an ongoing basis; (iii) emerging risks which can be temporary or recurrent and may at times need urgent intervention, including risks external to the regulatory framework but which are still relevant. While acknowledging these differences, RBS applies to all types of tasks and risks.

14. **RBS utilises relevant data to identify and assess patterns in financial markets**. It aims to understand and address the root cause of issues, to test risk hypothesis and intervene early. Root cause analysis is critical to the success of both risk-based and outcome focused supervision.

15. **RBS recognises the importance of supervisory judgement and experience**. Authorities' staff should be empowered to exercise their supervisory judgement and experience throughout the risk-based cycle, while applying clear criteria and objective measurements to ensure that assessments are based on solid rationale.

16. **RBS covers the entire supervisory landscape and does not solely address major risks and entities.** While prioritising based on risk prominence, all risks from the markets, sectors and firms under the authority's remit should be adequately mapped and periodically assessed, ensuring an appropriate level of supervisory coverage.

17. **RBS entails a level of risk acceptance/tolerance.** When prioritising risks, authorities focus their efforts on areas where the perceived risk is highest. This requires clear criteria to justify why certain risks are given priority over others, along with a well-defined understanding of what constitutes an acceptable level of risk. Nonetheless, RBS does not provide absolute assurances. It relies on a supervisory culture that acknowledges trade-offs, while ensuring that critical risks—particularly those affecting investor protection, financial stability, and the orderly functioning of markets—remain central to the authority's supervisory programme.

18. **RBS ensures adequate attention to risk treatment.** While ensuring sufficient time and quality to the identification and assessment of risks, authorities should maintain focus to addressing such risks through both proactive and reactive supervisory actions.

19. **RBS facilitates clear and considered communication** from senior management to supervisory staff, which enables leaders to articulate their vision and expectations more effectively, thereby shaping the strategic direction of the authority.

20. **RBS aids authorities' accountability and transparency**. It allows the communication of their key areas of focus, introducing a level of responsibility in delivering those objectives.

4 Foundational elements of risk-based supervision

4.1 Supervisory strategy

Effective risk-based supervision begins with a clearly defined supervisory strategy, which should align with the authority's broader strategic goals and outline the supervisory landscape, key objectives, and the tools and approaches to be used to achieve the stated supervisory objectives. Depending on their mandate, authorities will balance their objectives. The supervisory strategy should not favour one objective over another without justification but rather be responsive to the supervisory environment and adapt to emerging or materialising risks and challenges.

An authority's strategy is expected to support the development of a comprehensive risk tolerance or risk appetite statement. It is important that authorities develop a sense of their level of risk tolerance or appetite which considers parameters and assertions to differentiate between acceptable and unacceptable levels of risk, thereby allowing resources to be focused on those areas where there is the highest level of perceived risk.

Leadership bodies of authorities are ultimately responsible for the execution of the supervisory strategy and its communication to both internal and external stakeholders.

4.2 Risk assessment framework

Risk-based supervision is underpinned by a structured and coherent framework, characterised by appropriate people, processes, tools, scale and parameters that help its implementation. A structured risk assessment framework includes:

- A governance structure, ideally comprising sufficiently senior and experienced individuals with responsibility for overseeing the risk-based process, ensuring consistency and accountability throughout the implementation of the risk assessment framework.
- Developing methodologies and risk models. Without prejudice to the different supervisory areas, the use of consistent risk methodologies providing a standardised approach across the authority's supervisory remit, allows for consistency and comparability.
- Selecting parameters to categorise specific entities, groups of entities and sectors in terms of their supervisory importance, as the impact of the materialisation of a risk will depend on their size, scale and complexity.
- Establishing methods to evaluate and measure the impact and the effectiveness of past supervisory actions against identified risks in order to inform future risk identification and assessment exercises.
- Conducting regular evaluations of the risk-based process, employing different methods to ensure that both known and emerging risks are captured in the exercise.

5 Underlying phases

Risk-based supervision is typically implemented through several key phases. While these phases are presented in a structured format, authorities may adapt the sequence based on their specific needs and context.

To enhance clarity and applicability, risk identification (and partly risk assessment) is divided into industry-wide and entity-based components. Although entity-based identification, focusing on supervised entities, is the most common, other models may be more suitable in specific areas of financial market supervision. These include:

- Transaction-based identification, which uses data from specific transactions to detect risks like insider trading or market manipulation and guide supervisory focus.
- Product-based identification, which targets risks linked to specific financial products and how they may manifest on the market in question.

Authorities should choose the most appropriate model based on their national market and organisational structure. Nonetheless, core principles from the entity-based approach can be adapted to other models as needed.

5.1 Risk identification

Industry wide risk identification

An industry-wide risk identification exercise enables authorities to understand the external risk environment and assess its impact on markets, sectors and products under their remit. It also supports the identification of systemic risks that may disrupt services across borders.

Authorities should leverage internal expertise to analyse market conditions through scenario analysis and forecasting, considering macroeconomic, social, political, technological, environmental, legal and regulatory factors. To frame this analysis, several guiding questions may be posed, such as:

- How may the prevailing macro-economic conditions affect financial markets? (i.e., interest rates, inflation & economic growth).
- What are the anticipated technological developments that may affect market structures?
- Are there anticipated regulatory/legal amendments over the relevant period that may affect the market?
- How may the current and anticipated (national, EU, worldwide) political landscape affect financial markets?

In addition, several other techniques and processes can be employed to identify key risks, such as market research (using sources such as ESMA, ECB, IOSCO, IMF and OECD reports), workshops, brainstorming sessions to identify risks and initiate robust challenge/discussions. Working groups can also be utilised to discover detailed information about risks, including those from industry participants.

The output of the industry wide risk identification process should be a consolidated list of external risks which may influence an authority's supervisory remit over the coming supervisory cycle. The industry risk inventory should allow the formation of a comprehensive understanding of the risks' sources, root causes and consequences if they materialise.

Entity based risk identification

At a more granular level, entity-based risk identification aims to understand the risk profiles of entities and/or clusters of entities under the remit of the authority.

Authorities may choose to assess risks at the entity level, cluster level, or a combination of both. When supervising a large number of entities, it may be more efficient to focus detailed analysis on firms of greater size, complexity, geographical reach or systemic importance, while applying a thematic or cluster-based approaches to others. When utilising cluster-based risk identification it is important that authorities have a methodology for ranking or clustering entities with sufficiently similar features.

Effective risk identification requires supervisors to have a solid understanding of the entities' organisational structures, business operations and the markets in which they operate. This should be supported by both regulatory and third-party data sets and tools to help analyse this data. Supervisors will evaluate a range of elements at the entity level, including governance frameworks, financial resources, internal controls, IT systems, staffing levels and operational resilience, to detect where harmful or illegal behaviour may arise.

Supervisors can leverage these key elements of the supervised entity to extrapolate a set of risk areas or risk categories. Generally, a universal taxonomy of risk areas or risk categories (rather than an annual ad hoc identification of risks) allows to best compare similar entities within specific sectors.

The final output of the entity-based risk identification process should be a clearly defined list of risks applicable to entities or clusters. It should, also, includea narrative on the impact a materialisation would have on the entity/cluster, sector and/or wider market supported by data and/or evidence.

5.2 Risk assessment

Probability and impact scoring

Risk assessment builds on the identification phase by evaluating the probability of the occurrence and potential impact of identified risks. Authorities should assess risks using both qualitative and quantitative data, considering how industry-wide and entity specific/cluster elements interact. The same may also apply to other models, such as product or transaction-based assessments.

The assessment of risks should be done with a view to identifying potential risk scenarios and evaluating their criticality. The criticality of the risk scenario is represented by the risk score resulting from the probability and impact assessment. The calculation of this score can vary between authorities, however, typically it is a function (usually the product) of the two variables. The higher the risk score, the greater the perceived probability of materialisation and resulting impact on markets/entities.

Scoring risks supports comparability, prioritisation and objective evaluation. While numerical scoring is important for these purposes, expert supervisory judgement remains essential and should be applied consistently. Implementing quality assurance processes can help ensure that high quality judgements are made and there is not absolute reliance on numerical scores.

Authorities may adopt top-down (industry), bottom-up (entity) or hybrid approaches, provided they enable objective comparison across risk areas.

Industry-wide risk assessment

Authorities should assess each risk scenario by estimating:

- its potential impact on investor protection, financial stability, systemic risk or market integrity or/and any other harmful effects such as disruption of critical operations or unfair market conditions; and

- its probability of materialisation, focusing on factors or conditions that may hinder or facilitate its materialisation. Historical data may inform this assessment, but for emerging or novel risks, expert judgement is key.

The final score reflects the combined evaluation of these dimensions.

Entity-based risk assessment

An effective risk assessment at entity or cluster level builds on the entity risk identification undertaken in the previous phase. To undertake an effective entity-based risk assessment:

- The first variable, impact, should be evaluated based on potential consequences for supervisory objectives, market functioning, and the entity's own regulatory compliance.

This normally considers the entities' nature, size, complexity as well as market interdependencies (domestically and cross-border); and

- The second variable, the probability of a risk occurring, is informed by evaluating the governance of the entity, its internal controls, past incidents, complaints and other behavioural indicators. Supervisory judgement is crucial, especially where data is limited.

Following the assessment of these two variables, the risk score should be calculated.

Risk aggregation and reporting

The resulting risk scores (a function of probability and impact variables) can be aggregated to support prioritisation and resource allocation.

Authorities should consider establishing risk categories which correspond to the score obtained following the assessment of probability and impact. For example, rating scales (e.g. high, medium-high, medium-low, low) can be expressed in a risk matrix table to aid the visualisation and communication of risk categories.

Authorities should be cautious in placing absolute primacy in numerical ratings since the overall assessment of the risk score reflects not only quantitative judgements, but also qualitative ones about economic and market conditions, and other relevant factors, such as supervisory intelligence. For this reason, numerical ratings may create a misleading impression of precision about the level of risk that is not achievable in most cases.

Aggregation by risk area or entity provides different perspectives. Authorities may develop individual profiles for large entities and consolidated profiles for clusters of smaller ones. Authorities should remain aware of the limitations of aggregation, ensuring that individual risk analyses are considered when planning interventions.

5.3 Risk prioritisation and treatment

Prioritisation of risks

Following identification, assessment and aggregation, authorities must determine which risks to prioritise, re-prioritise, or de-prioritise. Authorities' senior management play a central role by fostering a culture that supports informed trade-offs and empowers staff to make difficult decisions.

Prioritisation should be based on clear, well-founded criteria that ensure consistency and integrity. It is imperative that these criteria are both well founded and utilised to protect the integrity and consistency of the prioritisation process. While models and scoring systems support decision-making, supervisory judgement remains essential due to inherent uncertainties and information asymmetries. Authorities should be cautious not to rely mechanistically on mathematical models as they may give a false sense of accuracy.

Authorities may apply various prioritisation criteria, tailored to their structure and market context. These include:

- **severity** (based on impact and probability scores, considering both domestic and cross-border implications);
- **coverage** (to ensure all areas within the supervisory remit receive appropriate attention over time);
- the emergence of **new risks** (such as innovative products or entities requiring early scrutiny);
- **urgency** (to enable swift responses to immediate threats and prevent escalation); and
- **strategic direction** (prioritising risks linked to the authority's broader goals, e.g. promoting retail market participation by addressing risks like market manipulation or excessive fees).

Reprioritisation

Risk prioritisation is a dynamic process, subject to change as new concerns arise or existing risks evolve. Authorities should continuously monitor risks, setting up specific monitoring processes using diverse sources and tools.

As new supervisory issues can arise throughout the relevant period, these should be considered, adjusting priorities as needed to remain agile and respond effectively throughout the supervisory cycle.

To support this adaptability, authorities should ensure that their resource allocation is reflective of the evolving risk environment and that supervisory plans have sufficient flexibility to deploy focus and capacity to emerging issues.

Supervisory work plans (development and implementation)

Authorities should translate prioritised risks into supervisory work plans, setting timelines, and allocating resources in line with their risk appetite and strategic objectives. Work plans should balance ongoing desk-based supervision with targeted on-site inspections, tailored to entity-specific conditions, risk profiles, and the overall supervisory environment.

The execution of the supervisory work plan should be monitored regularly, with updates provided to senior management. External communication of supervisory priorities, where appropriate, should be considered to enhance transparency, manage expectations, and foster collaboration with supervised entities.