ESMA
European Securities and Markets Authority

12 June 2025
ESMA42-1710566791-6103

Principles on third-party risks supervision

Table of Contents

1 Introduction

1.1 Background

1. Most supervised entities across EU securities market sectors within ESMA's remit (the entities) rely on third parties to provide them with services, business functions, processes and products (the services). Traditionally, these types of services were mostly provided in the context of an outsourcing arrangement and market regulators focused their expectations and supervisory approaches on outsourcing practices. [1] The digitalisation of securities markets has increased supervised entities' dependence on third parties. This requires supervisors to expand their approach to the enlarged scope of third-party risks. There can be significant heterogeneity in these practices, as, for example, the supervised entity (the entity), can use third-party service providers (the third-party) in relation to services of varying scope and criticality, the third-party can belong to the same group as the entity or not, can be located in the EU or outside it, and be regulated or unregulated.

2. The use of third-party services may bring benefits to the entity, such as new or higher quality services, dedicated expertise and reduced costs arising from economies of scale. At the same time, deciding to use a third-party may also bring risks (third-party risks) such as a loss of control, non-compliance with regulatory provisions, reduced operational resilience, security issues and exposure to concentration risks. In this respect ESMA and NCAs have observed the increasing use of third parties by entities under their supervisory remit.

3. As a result, it is important that third-party risks are adequately supervised across all EU jurisdictions to create a robust and efficient EU securities market. For that, consistent and effective supervision of third-party risks across sectors within ESMA's remit, in compliance with the relevant EU legal framework and considering specificities of the different sectors and heterogeneity in the forms and types of services provided, should be promoted. Considering ESMA's role in "building a common Union supervisory culture, and consistent supervisory practices"[2], ESMA developed these principles on third-party risk supervision (the Principles) to contribute to these objectives. This common framework provides an opportunity for ESMA and NCAs to foster a consistent and streamlined approach across sectors and focusing on the efficient allocation of resources. Establishing a common baseline supports a level playing field and further supervisory convergence work in this area.

4. The provision of a service by a third-party can encapsulate different terminology and naming conventions depending on the sector, contractual arrangements and techniques used. For the purposes of these Principles, reference to "third-party services" encompasses any term used in relevant sectoral legislation to refer to outsourcing, delegation or other forms of provisions of services by a third-party performed on a recurrent and ongoing basis.

[1] Generally understood as referring to an arrangement between an entity and a third-party service provider, to perform a service on a recurrent or an ongoing basis, that would otherwise be undertaken by the entity itself.
[2] These Principles are issued under Article 29 of ESMA Regulation, Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 which enables ESMA to develop new practical instruments and convergence tools such as principles. Principles set out high level supervisory guidance and expectations on broad cross-sectoral topics, in order to provide common frameworks, objectives, and/or criteria. The content of Principles is not subject to any 'comply or explain' mechanism for National Competent Authorities (NCA) and is non-binding.

1.2 Purpose and scope

5. The Principles provide guidance to supervisory authorities to identify, assess and supervise the third-party risks of EU entities operating in securities markets, in compliance with the relevant legal framework while applying the principle of proportionality.

6. The Principles take into account and are consistent with established international standards (IOSCO[3], FSB[4], BCBS[5]).

7. The Principles apply across EU securities markets within ESMA's remit [6], including ESMA's direct supervision mandates. They provide a common framework on third-party risks which aids authorities in applying the relevant EU regulatory requirements, as well as guidance issued by ESMA and the other European Supervisory Authorities (ESAs)[7]. Important to note that the management of ICT risk and the use of third-party service providers to provide ICT services fall under the scope of the Digital Operational Resilience Act (DORA) and are therefore out of scope of these principles. At the same time, these principles have considered and align with DORA third party risk management requirements.

8. In particular, the Principles aim to support supervisors in performing effective risk-based supervision of entities using third-parties when existing legislation remains high-level on all or on some aspects. For those regulatory frameworks that already imposes specific requirements on the use of third-party services, these requirements would prevail over these Principles.

9. The Principles are non-binding. They intend to fit into supervisory authorities' risk-based, data driven and outcome-focused supervisory approaches. Supervisory authorities should apply the Principles in a proportionate manner, having regard for the size and overall risk profile of the entities, having consideration to the nature, scale and complexity of their services, activities, products and operations and potential effects on investor protection, financial stability, and orderly markets.

10. The Principles apply to all types of third-party arrangements, whether the third-party belongs to the same group or not, is located in the EU or in a third-country, and independently from the underlying technology that might be used to provide the service. In addition, specific risks or situations are addressed under section 2.4 (third-party located in a third country[8], intragroup arrangement[9], supply chain[10], use of third party for internal controls[11], access and audit rights[12]).

11. The main focus of the Principles is on critical activities. The extent of reliance on third-party services can vary significantly from one entity to another. For example, the use of third-party services can be extensive and / or relate to services considered critical, or playing a material role in the running of the entity's activities. It should be noted that, while focus can be set on

---

[3] Principles on Outsourcing in October 2021, Principles for financial market infrastructures in April 2012
[4] Enhancing Third-Party Risk management and Oversight 4 December 2023
[5] Principles for the sound management of third-party risk – Consultative document – July 2024
[6] All relevant activities of competent authorities carried out pursuant to the Union acts referred to in Article 1(2) of the ESMA Regulation (ESMA Regulation - Regulation (EU) No. 1095 /2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC).
[7] E.g. EBA Guidelines on outsourcing arrangements
[8] Principle 10.
[9] Principle 11.
[10] Principle 12
[11] Principle 13.
[12] Principle 14.

the use of third-party services for such critical activities, using third-party services for non-critical activities may also create substantial risks. For the purpose of these Principles, reference to "critical" activities encompasses any term used in relevant sectoral legislation or any situation assessed by the entity and / or by the supervisor to identify activities or functions where a defect would materially impair the entity's compliance, financial performance, soundness or continuity.

12. The abovementioned concepts apply to the entire set of Principles set out in this document and are not specifically repeated under each principle.

2 Principles

2.1 Principle on the supervisory overview

Principle 1: Supervision of third-party risks

13. While the responsibility for the use of a third-party service provider lies with the supervised entity, supervisory authorities should effectively supervise entities' exposure to third-party risks. For this purpose, supervisory authorities should ensure that reliance on third parties does not impair the depth nor effectiveness of their supervision[13].

14. In particular, supervisory authorities should promote that entities have appropriate governance and risk frameworks in place to identify, manage and oversee third-party risks and that entities are not operating as "empty shells"[14].

15. Supervisory authorities should assess the third-party risks when the entity requests an authorisation or registration to operate and upon notification of specific arrangements or material changes when such notification requirements exist. In particular, the supervisory authorities should identify whether third-party arrangements result in a material change to the conditions and obligations of the entity's initial authorisation or registration to operate. Under the conditions set out in the relevant regulatory framework, the supervisory authority may refrain from authorising, registering or approving the entity or the arrangements in case of concerns in the use of third-party services.

16. Supervisory authorities should also embed third-party risks into their on-going supervision methodologies and in their desk-based and on-site supervisory activities. On the basis of such an assessment, the supervisory authorities are expected to reflect the risks posed by the entities' use of third parties in their regular risk assessment and supervisory activities. When relevant, the supervisory authorities should assess the overall reliance of an entity on third

[13] E.g. in case of empty shell or third party located outside the EU (see principle 10)
[14] Also called "letter box entities" in some EU legislations, see e.g. under AIFM framework

parties and the related risks posed to its corporate substance as well as on the effectiveness of the governing bodies' oversight in this area.

17. When supervisory authorities are concerned about the use of third parties by the entities and their resulting ability to comply with and meet the objectives of the relevant legislations, they should intervene with relevant supervisory measures.

18. Supervisory authorities should maintain an overview of the relevant third-party arrangements to be able to identify and monitor potential concentration risks.

2.2 Principles on the supervised entity

Principle 2: Effective governance to manage third-party risks

19. Supervisory authorities should ensure that reliance on third parties does not impair the exercise of independent decision-making and effective governance of the entity and its ability to comply at all times with EU laws and regulations.

20. Boards (administrative and/or supervisory), senior management and the management body (thereafter altogether the governing bodies) of EU supervised entities cannot delegate their tasks and responsibilities in terms of oversight, management and decision-making. The governing bodies are responsible for the well-functioning of all activities of the supervised entity and should take all necessary steps to discharge their legal obligations, regardless of the use of third parties by the entity.

21. Similarly, due to their significant influence over the direction of the entity, the delegation of key function holders'[15] roles and responsibilities is usually regarded as inconsistent with the need to uphold decision-making and effective governance in the entity[16] (see also Principle 13 on the use of third parties for internal control functions).

[15] Unless already defined by sectoral legislation, key functions holders generally include e.g. heads of internal control functions, heads of important business lines or entities, Chief Risk Officers, Chief Financial Officers, Chief Information Officers ((as well as equivalent senior managers positions with direct reporting line to the Board.

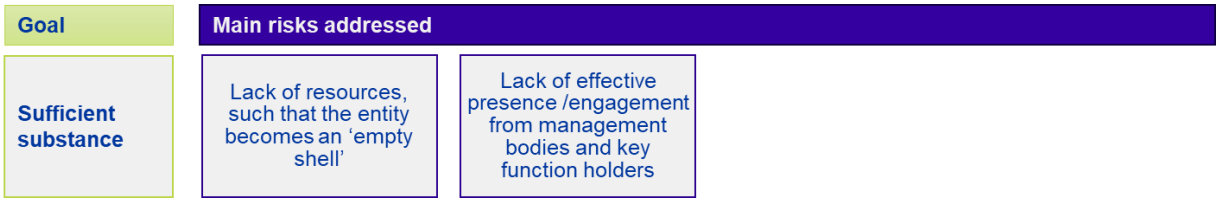
[16] It is however recognised that there are certain specific cases where exception has been granted explicitly by sectoral legislation.

Principle 3: Oversight of third-party risks by management bodies

22. Supervisory authorities should ensure that entities' governing bodies are accountable for maintaining effective oversight[17] of the third-party risks the entity is exposed to.

23. Supervisory authorities should check that members of the governing bodies have appropriate skills and competences to understand how third-party risks affect the entity's risk profile and effectively manage, challenge and oversee the risks related to the activity provided by the third-party. Supervisory authorities should also check that members of the governing body seek and receive regular and relevant management information for that purpose. Where the entity uses a third-party for critical activities, and/or to a significant cumulative extent, and considering the entity's size and overall risk profile, the supervisory authority should promote that a member of the governing body is responsible (e.g. executive board member, senior manager, head of department) for the third-party risk management and the implementation of an appropriate oversight framework.

Principle 4: Sufficient substance



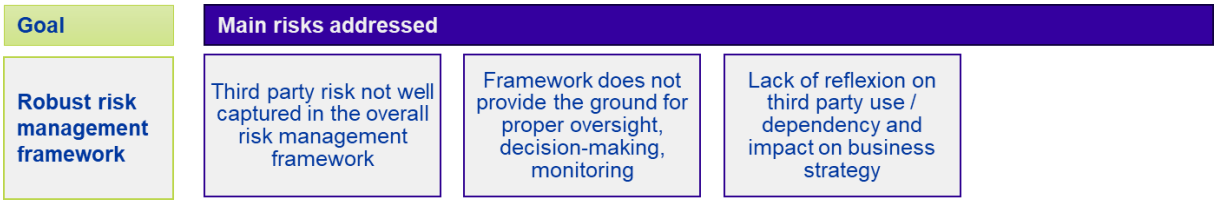
24. Supervisory authorities should check that the entity maintains – at all times – sufficient corporate substance, through appropriate human and technical resources as well as adequate governance, control, transparency and accountability frameworks. The risk related to insufficient substance depends in particular on the criticality and the number of activities undertaken by third parties. The assessment of sufficient substance may evolve as the entity grows and develops its business. Supervisory authorities should consider whether there is sufficient time commitment and meaningful effective presence of the governing bodies and staff within the EU. For instance, the CEO, and other members of the governing bodies should effectively be located in the EU on a regular basis to fulfil their responsibilities. The same should apply to key function holders.

25. To support this, in particular when remote working is used, the supervisory authority should ensure that the entity determines rules that ensure staff sufficient availability, effective engagement and appropriate presence. The use of third parties should not lead to a situation

[17] Depending on the relevant sectoral legislation oversight responsibility may also be attributed to or share with other functions, such as the oversight function.

in which an entity becomes an ‘empty shell’, thereby affecting the conditions for its effective supervision.

Principle 5: Risk management framework



26. Supervisory authorities should check that the entity’s governing bodies establish and deploy, in cooperation with the function responsible for risk management, a robust third-party risk management, as a part of the overall risk management framework. The purpose is to ensure that third-party arrangements are well governed and do not create undue risks nor impair the quality and independence of the entity’s internal controls or their ability to oversee and supervise the risks and the compliance with legislation and guidance nor alter the entity’s relationship and obligations towards clients.

27. Accordingly, this third-party risk management framework should be operational, effective and comprehensive. To this end, it should provide clarity on reliance on third parties, setting out a basis for the oversight of third-party risk overall and of specific arrangements. It should also typically encompass: controls in relation to the use of the third-party (including limitations related to the supply chain where relevant), the conduct of comprehensive risk assessment(s), the contractual arrangements and the monitoring of third-party arrangements decision-making and reporting processes. For this purpose, the third-party risk management framework may impose more stringent requirements and closer monitoring for some activities, depending on their criticality and importance. Similarly, its level of granularity may vary depending on the third-party risks level considered acceptable by the entity.

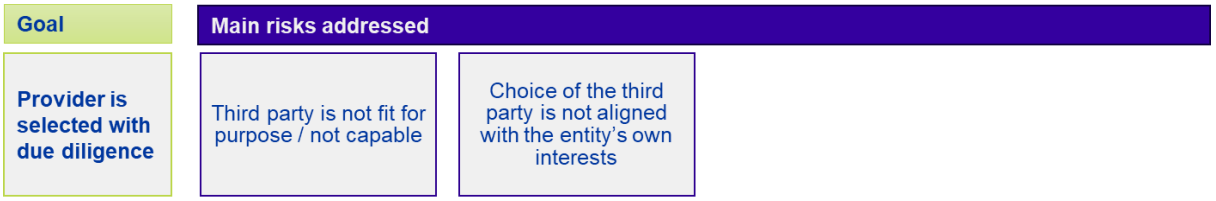
28. Where an entity significantly uses third parties, and considering the entity’s (evolving) size and overall risk profile, supervisory authorities should check it has in place a documented strategy on the use of third-party services. To support its effectiveness and credibility, this strategy is expected to be aligned with the business strategy and to form the basis of the third-party risk management framework. The third-party strategy and risk management framework documents should be reviewed regularly by the entity (at a frequency commensurate to the size and overall risk profile of the entity).

Principle 6: Risk assessment

29. The decision to enter into a third-party arrangement should be preceded by a documented assessment of the risks, benefits and costs of a potential arrangement and, when applicable, of its alignment with the third-party strategy. To this end, supervisory authorities should challenge and assess the quality of the risk assessment by the entity. A risk assessment should typically cover all relevant elements of the third-party arrangement, such as the impact of the third-party arrangements on the business model and consistency with the strategy on the use of third-parties, their criticality and importance, possible location, impact on business continuity planning and available exit strategies, risks of losses (of knowledge, control, etc.), supply chain related risks (Principle 12), potential impact on reputation, operational efficiency, security of data and systems, including clients' related information and level of dependency on a third-party (including at entity/group level). The depth of such assessment and the frequency of its review is expected to be commensurate to the criticality and importance of the activity.

2.3 Principles on the relation with the third-party

Principle 7: Due diligence



30. Supervisory authorities should ensure that the entity conducts comprehensive due diligence checks on the prospective third-party(ies) (including any relevant sub-provider(s) of the supply chain) before entering, amending or renewing an arrangement. Effective assessments to this end consider all relevant elements, such as, amongst other points: the third-party business model, nature, scale, complexity, financial situation, ownership and group structure, the entity's processes and procedures, resourcing (people and technology), its regulatory status, reputation, whether the third-party provides the same service to other group entities, (when available) its past performance in services provided, whether it belongs to the same group and the influence and control over it (see Principle 11 on Intragroup arrangements), location (or location of data) (see Principle 10 on third-party location), possible conflicts of interest, risk management and internal controls put in place by the third-party and their alignment with the entity's own risk management framework.

    Supervisory authorities should check that the entity conducts and documents due diligences on a regular basis throughout the lifecycle of a contract and when relevant circumstances arise (e.g. in case of reputational issues or known incidents affecting the third-party).

Principle 8: Contractual arrangements

Goal	Main risks addressed			
Formalisation is fit to ensure legal certainty	Arrangement is misaligned with the entity's own risk management framework/strategy	Aspects are missing / do not provide a good basis for a good quality of service / monitoring	Level of details is not adapted to the criticality of the service for the entity	Contract/SLA do not include the relevant mitigants to the risks identified

31. Supervisory authorities should request that third-party arrangements are formalised through written contracts and service level agreements (SLAs) to be reviewed on a regular basis. The level of details of the arrangements may vary depending on the criticality of the service provided to the entity. Supervisory authorities should ensure that the entity has considered the risks identified during the risk assessment process in the arrangements. They should include all necessary elements to offer sufficient legal certainty on the obligations and rights, responsibilities and expectations of all parties during the contract life, to end and/or renew it as well as in case of dispute resolution. The arrangements should explicitly grant audit rights for the entity, its auditors and the relevant EU supervisory authorities. The arrangements should provide a contractual basis for the monitoring and control of the activity provided by the third-party (with clearly defined service level, performance indicators and reporting processes), business continuity, including record retention, entity's termination rights and exit plans to ensure that, post-termination or otherwise whenever necessary due to failures on the third-party's part, the entity can terminate or exit the contract with no ongoing remaining regulatory, operational or technological dependency on the third-party.

32. Supervisory authorities should promote that SLAs are defined at entity level and not only at group level. As applicable, SLAs should also include the place where the activity is going to be conducted (i.e. city and country) and updated as need be.

33. Supervisory authorities should check the arrangements are clear on whether supply chain is allowed by the entity and, if so, for which activities and under which conditions (e.g. pre-approval by the entity).

Principle 9: Effective monitoring

Goal	Main risks addressed		
Monitoring of the arrangement is effective	Monitoring capacities insufficient or not adapted to the criticality of the service for the entity	Monitoring is not effective, regular, risk-based	Service provided by third party is not embedded in the internal controls' framework

34. Supervisory authorities should promote that the entity remains responsible for retaining an adequate number of staff with the relevant knowledge and skills to effectively monitor the third-party arrangements. The resources allocated to the monitoring should be commensurate to the criticality of each activity for the entity and/or of its complexity and should be aligned with relevant exit strategies and plans when they foresee the possibility to bring the service in house in case of disruption or termination.

35. Supervisory authorities should check that the entity conducts regular monitoring of the performance of the third-party's duties, in light of the written contracts, SLAs and the entity's own risk management framework and internal control functions' plans. The monitoring should be done on an ongoing basis, the three lines of defence or other internal controls' model used by the entity should be applied and possible adjustments should be considered in case of specific risks or circumstances (e.g. incidents).

36. Where the risks, nature, scale or complexity related to the arrangement materially changes, the applicable monitoring and controls should be re-assessed. Supervisory authorities should ensure that reports on the monitoring and control activities of the regulated entity and on any adverse development arising in any third-party arrangement are reviewed by its governing bodies and are communicated to the service provider. Supervisory authorities should promote that in this context, regular monitoring includes periodic on-site visits and periodic checks to ensure that the activity is delivered at the quality and under the conditions agreed and remains adapted to the entity's expectations and needs.

2.4 Principles on specific risks and issues

Principle 10: Third-party location[18]

Goal	Main risks addressed	
Impact of provider Location (out of EU) is mitigated	Provider cannot be well monitored / supervised due to its location	Risks related to the location have not been well identified / assessed

37. While the EU's framework and supervisory architecture supports the application of a common framework and facilitates cooperation of supervisors to perform their tasks, the location of the third-party in a third country may expose the entity to specific risks.

38. The supervisory authority should check that these specific risks are considered in the risk assessment, due diligence, decision-making and monitoring processes by the entity.

39. When the third-party (or a service provider in the supply chain) is located in a third country, supervisory authorities should promote that the entity considers the specific risks and conditions in the third country, and in particular:

- The local regulatory framework and effective enforcement of the law in third country,
- The entity's ability to comply with EU applicable regulatory requirements, initial conditions of registration/authorisation and other supervisory expectations,
- The entity's ability to identify, oversee and manage the risks,

[18] To the extent outsourcing outside EU/EEA is permitted by sectorial legislation and ESMA guidance on those matters.

- The presence of appropriate contractual arrangements for unrestricted supervisory access.

40. The supervisory authority should also check that the location of the third-party in a third country does not impact its ability to supervise the activity. For this purpose, when the activity provided by the third-party requires an authorisation to operate or registration if performed in the EU, the supervisory authority should verify that the third-party is regulated and supervised by a relevant supervisory authority in that third country. The supervisory authority should also promote that there is an appropriate cooperation agreement (e.g. in the form of a memorandum of understanding, college agreement, etc.) with the supervisory authorities responsible for the supervision of the third-party.

Principle 11: Intragroup arrangements

41. Entities belonging to a wider group may use intragroup arrangements to benefit from economies of scales and/or higher level of expertise.

42. Intragroup arrangements may carry different types of risks than those situations where an external third-party is used. The level of the risks and their type depend on the specificity of each situation to be assessed on a case-by-case basis in the risk assessment process. Supervisory authorities should check that the entity addresses these risks. To better capture the intragroup impact on the risks assessment, the following risks may be considered: (i) potential conflicts of interest; (ii) the extent of control and influence that may be exercised by the third-party over the supervised entity; (iii) the location of the third-party, whether it is in the same country or in the EU compared to outside of the EU; (iv) whether the third-party is regulated or unregulated.

43. Supervisory authorities should check that the entity can (i) maintain autonomy and make its own decision on whether to use the third-party or not, (ii) obtain a service adapted to its own business needs and activities on an on-going and timely basis, and (iii) have the opportunity to apply mitigants. In this respect, supervisory authorities should check that the entity's governing bodies are committed towards the entity, through (i) a formalised contractual relationship directly with the entity, (ii) sufficient time allocation and (iii) financial compensation or remuneration paid by the entity.

44. When the entity uses intragroup or centralised services (e.g. through a master agreement), it is recognised that the entity may rely, to the extent that it is relevant, on processes undertaken centrally (pre-assessment of the risks, due diligence, standard contract, and SLA, standard KPIs). However, the supervisory authority should ensure that the entity retains full ownership (i) of the decision to enter into such an arrangement and (ii) of the underlying risks. For instance, the supervisory authority should review that the entity is able to complement and challenge as relevant such centralised pre-filled processes and that all risks related to its specific situation and needs are appropriately captured and mitigated.

Principle 12: Supply chain

Goal	Main risks addressed
Risk management & controls extend to relevant supply chain actors	Loss of control and oversight

45. The oversight of third-party arrangements can be complicated by the use of sub-contracting in the supply chain, whereby the third-party transfers the performance of an activity, or part of it, to another third-party. This can increase the risk of loss of oversight and control by the entity, in particular in case of a long or complex chain. Therefore, supervisory authorities should check that appropriate safeguards are put in place by the entity, such as setting limits and conditions on the type and (part of) activity that can or cannot be sub-contracted[19]. Supervisory authorities should also check that entities integrate the supply chain elements in their risk assessment and due diligence process, and in the respective appropriate clauses in the written arrangements (see Principle 5 on risk management framework). Such arrangements should ensure that, at least20, the entity is informed in case a critical activity (or part of it) is transferred by the third-party to another sub-party and that the entity has a role in decision on the sub-provider and its location.

46. If sub-providers are involved in critical activities, supervisory authorities should check that the entity can challenge the sub-provider and carry out respective due diligence. The arrangements should ensure that the monitoring and oversight by the entity, as well as the audit and access rights by the entity, its auditors and EU supervisory authorities remain effective, including at the sub-provider location.

Principle 13: Use of third parties for internal controls

Goal	Main risks addressed	
Internal controls remains fully owned	Independence and segregation of functions not respected	Loss of control / visibility / ownership on the internal controls

47. The entity's governing bodies are, at all times, fully responsible and accountable for the setting of the entity's strategies and policies and for the oversight of their implementation. Supervisory authorities should check that, when using third parties, the entity keeps ensuring appropriate segregation and independence of its internal control functions, such as risk management, compliance, and internal audit function, according to the three lines of defence or other applicable internal control model[21].

48. Supervisory authorities should check that the entity pays attention to maintaining sufficient substance and to retaining its responsibilities, visibility and control (see Principle 4 on sufficient

[19] Including, but not limited to, those limited by sectoral legislation.
[20] Prior formal approval may be relevant in some situations, for example when required by sectoral legislation.
[21] In the case of use of third-parties, the agreed third-party risk management framework implementation (e.g. risks assessment, due diligence, monitoring) should not be entrusted to a third-party.

substance) when assessing the use of a third-party to undertake a significant part of any of their internal control functions. Therefore, the reliance on third parties for internal control functions is expected to be duly justified and commensurate to the size and overall risk profile of the entity and its activities. While, when allowed by sectoral legislation, a supervisory authority might consider the use of a third-party for internal control activities reasonable for entities with lowest risk considering their size and overall risk profile, such assessment should carefully consider the potential systemic impact of the entity and potential impact on its customers. Supervisory authorities should ensure that, as the entity grows and gains in maturity, it reconsiders the extent of such arrangements.

49. Supervisory authorities should ensure the entity introduces exit strategies and plans, measures, controls, processes and reporting arrangements so that the provision of internal control activities by a third-party does not impair the effective functioning of the entity and the quality of the entity's controls. These may include limits to the extent of the control function is carried out by a third-party.

Principle 14: Access and audit rights

Goal	Main risks addressed
Access & audit rights are granted to the entity & (N)CA	Activity becomes unsupervisable / inaccessible to entity & supervisor

50. Supervisory authorities should check that the entity ensures that there is no obstacle to the effective oversight, access and audit rights of the third-party by the entity, the entity's auditors, the relevant EU supervisory authorities of the supervised entity (see Principle 10 on third-party location). In relation to the services provided to the entity, supervisory authorities should be able to have access to, as necessary, information, data, IT systems, premises and personnel of third-party as well as relevant sub providers of the supply chain.