JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2025 85
4 December 2025

Joint ESAs Report in response to the European Commission consultation pursuant to Article 58(3) of Regulation (EU) 2022/2554 (DORA)

Executive Summary

This report presents the joint response of the European Supervisory Authorities (EBA, EIOPA and ESMA) to the European Commission's request under Article 58(3) of Regulation (EU) 2022/2554 (DORA) to assess whether statutory auditors and audit firms should be subject to strengthened digital operational resilience requirements by means of its inclusion in the scope of DORA or by means of amendments to Directive 2006/43/EC.

The report provides an overview of the regulatory framework applicable to the statutory auditors and audit firms, including the limited role played by the ESAs in the context of their supervision.

Furthermore, the report reflects on the role played by the statutory auditors and audit firms in the financial sector, the financial market and more broadly in the economy in general, as they provide independent assurance on the accuracy and completeness of financial statements, including those of public-interest entities, contributing to market transparency, investor protection and financial stability.

The report reflects on the fact that confidentiality, integrity and availability of information accessed during audits is critical: disruption in audit processes may have reputational and regulatory consequences for the auditee. However, audit activities do not form part of the operational value chain of the auditee and therefore do not directly affect the continuity of financial or other services.

Finally, the report reflects on the implications of extending the scope of DORA to statutory auditors and audit firms. Those implications are assessed according to multiple dimensions:

a) Market perspective. The EU audit market is highly concentrated; inclusion of statutory auditors and audit firms in the scope of DORA could raise fixed costs and reinforce concentration, limiting audit choice and conflicting with competition and administrative burden reduction objectives.

b) Auditees' perspective. Extending DORA requirements to auditors could increase audit fees. The added value of higher resilience safeguards may not outweigh the cost impact for the audited entities.

c) Supervisory perspective. National audit oversight authorities would require significant re-skilling to supervise DORA compliance.

d) Implementation & governance perspective. Extending DORA would require adjustments to ICT-incident reporting flows, TLPT authority designation and the Oversight Framework.

e) Cooperation between authorities. Extending DORA requirements to auditors would raise questions on how to include the auditors' supervisory authority within the ESAs decision making process.

f) Inclusion of service providers in the scope of DORA. Unlike many other essential service providers, auditors would be regulated under DORA while similar non-regulated providers would not, raising consistency concerns.

In addition to these implications, the report reflects on the fact that to carry out their statutory tasks, auditors need to access auditees data, which need to be properly protected by measures defined both by the Auditee and the Auditors, providing examples of those measures.

Finally, the report concludes with the ESAs opinion that the identified implications of the application of DORA to the statutory auditors and audit firms appear to outweigh the potential benefits. The ESAs therefore consider that including statutory auditors and audit firms within DORA's scope is not warranted at this stage.

Legal basis and mandate

1) This report sets out the joint response prepared by the European Supervisory Authorities (ESAs) (the European Banking Authority – EBA, the European Insurance and Occupational Pensions Authority – EIOPA, and the European Securities and Markets Authority – ESMA, hereinafter collectively "the ESAs") to the request of the European Commission pursuant to Article 58(3) of Regulation (EU) 2022/2554 (DORA).

2) Under this provision, the Commission, after consulting the ESAs and the Committee of European Auditing Oversight Bodies (CEAOB), shall by 17 January 2026 carry out a review and submit a report to the European Parliament and the Council on the appropriateness of strengthened requirements for statutory auditors and audit firms as regards digital operational resilience, by means of the inclusion of statutory auditors and audit firms into the scope of DORA or by means of amendments to Directive 2006/43/EC.

3) Therefore, on 29 October 2025, the European Commission sent a request to the ESAs for that purpose. The Commission's request was accompanied by a technical paper outlining the rationale for a potential inclusion of statutory auditors and audit firms within DORA's scope, describing the Union's audit supervision model, and asking the ESAs whether, in due course and in light of the broader DORA review, such an extension should be considered.

4) In their answer, as per the European Commission's consultation request, the ESAs focus on statutory auditors in the context of the Statutory Audit Directive (Directive 2006/43/EC) and Regulation (EU) No 537/2014 on specific requirements regarding statutory audit of public-interest entities.

Structure of this report

5) This report sets out the ESAs response to Commission's request and it is structured in the following sections:

   a. High-level overview of the regulatory framework applicable to statutory auditors and audit firms and responsibility of the ESAs;

   b. Role of statutory auditors and audit firms in the financial ecosystem and importance of their digital operational resilience;

   c. Potential implications of extending the scope of DORA to statutory auditors and audit firms;

   d. Conclusion and answer to the Commission's question.

High-level overview of the regulatory framework applicable to statutory auditors and audit firms and responsibility of the ESAs

6) The EU regime concerning statutory auditors and audit firms is primarily governed by the Statutory Audit Directive (Directive 2006/43/EC) and Regulation (EU) No 537/2014 on specific requirements regarding statutory audit of public-interest entities. These legal acts: (i) set the organisational, independence and quality-assurance requirements for statutory auditors and audit firms; (ii) assign oversight to national competent authorities; and (iii) establish the Committee of European Auditing Oversight Bodies (CEAOB) as the EU-level cooperation framework.

7) The Transparency Directive (Directive 2004/109/EC - TD) establishes requirements in relation to periodic (annual and half-yearly) issuer financial reports. Annual financial reports include financial statements subjected to audit. The TD further establishes national competent authorities' cooperation with ESMA, in line with ESMAR art 1(2).

8) Beyond audit law, Regulation (EU) 2023/2859 (ESAP) entrusts ESMA with establishing and operating the European Single Access Point for public financial, non-financial and sustainability-related information. The ESAP will serve as a central platform for publicly disclosed information related to statutory auditors and audit firms, including transparency reports produced by the auditors (Article 13 of Regulation (EU) No 537/2014).

9) Within this framework, the EU audit oversight is centred on national authorities defined by Member States according to Directive 2006/43/EC and Regulation No (EU) 537/2014, with specific provisions applicable to auditors in charge of public-interest entities. An EU framework for cooperation is established through the CEAOB, where ESMA is a member (without voting right), while EBA and EIOPA participate as observers.

European Banking Authority (EBA)

10) The mandate of the EBA, established by Regulation (EU) No 1093/2010, sets out the scope of actions and the powers of the authority to improve the functioning of the internal market by ensuring high-quality, effective and consistent regulation and supervision of several financial entities, including credit institutions, investment firms, payment institutions and electronic money institutions. Although the financial statements of such institutions are subject to statutory audit, and notwithstanding the fact that the scope of action of the EBA relates with

the field of auditing and financial reporting of the financial entities in its remit (Article 1(3) of Regulation (EU) No 1093/2010), almost all competent authorities in the remit of the EBA[1] do not have direct supervisory powers over statutory auditors or audit firms. In any case, given the importance of an effective dialogue between banking supervisors and statutory auditors, as stated in Article 12(2) of Regulation (EU) No 537/2014, EBA published in 2016 a set of Guidelines on communication between competent authorities supervising credit institutions and the statutory auditor(s) and the audit firm(s) carrying out the statutory audit of credit institutions (EBA/GL/2016/05).

European Insurance and Occupational Pensions (EIOPA)

11) The mandate of EIOPA, established by Regulation (EU) No 1094/2010, similarly to the one of EBA, sets out the scope of actions and the powers of the authority to improve the functioning of the internal market by ensuring high-quality, effective and consistent regulation and supervision of insurance and reinsurance undertakings, institution for occupational pensions and insurance and reinsurance intermediaries. Although the financial statement of these types of institutions is typically subject to statutory audit and notwithstanding the fact that the scope of action of the EIOPA relates with the field of auditing and financial reporting of the financial entities in its remit (Article 1(3) of Regulation (EU) No 1094/2010), almost all competent authorities in the remit of EIOPA[2] do not have direct supervisory powers over statutory auditors or audit firms. In any case, given the importance of an effective dialogue between insurance and reinsurance supervisors and statutory auditors, as stated in Article 12(2) of Regulation (EU) No 537/2014, EIOPA published in 2017 a set of Guidelines on Facilitating an Effective Dialogue between Insurance Supervisors and Statutory Auditors (EIOPA-BoS-16/071). Finally, it is also noted that Directive 2009/138/CE (Solvency II) includes three specific Articles disciplining respectively the requirements for undertakings to have at least the balance sheet included the solvency and financial condition report subject to Audit (Article 51a for individual undertakings and 256c for groups) and the duties of Auditors (Article 72).

European Securities and Markets Authority (ESMA)

12) The mandate of ESMA, established by Regulation (EU) No 1095/2010, includes fostering supervisory convergence and ensuring consistent application of EU law in areas such as the Transparency Directive (Directive 2004/109/EC) to ensure investors have access to comparable and up-to-date information about a company's financial position, ownership and governance. In addition, ESMA's responsibilities extend to activities closely linked to its core functions such as financial reporting and auditing. Given the close interaction between these areas, ESMA plays a slightly more prominent role[3] than the other ESAs by being member of the CEAOB without voting right, while EBA and EIOPA are observers.

13) While the three ESAs consider the statutory auditors' work as instrumental to support the supervision of financial entities (in case of ESMA, also to enhance market transparency and

[1] Exceptions are Commission de Surveillance du Secteur Financier (CSSF) in Luxembourg, Financial Market Authority in Liechtenstein and Finanstilsynet in Norway.
[2] Exceptions are: AFM in the Netherlands, Financial Market Authority in Liechtenstein and Finanstilsynet in Norway.
[3] In addition some authorities have direct supervisory powers over statutory auditors or audit firms: AFM in the Netherlands, Commission de Surveillance du Secteur Financier (CSSF) in Luxembourg, CONSOB in Italy, Financial Market Authority in Liechtenstein and Finanstilsynet in Norway.

accurate information), they do not have powers or mandates on the supervision of statutory auditors and audit firms. Therefore, the remaining two sections draw on publicly available information rather than on collected empirical evidence.

Role of statutory auditors and audit firms in the financial ecosystem and importance of their digital operational resilience

14) Statutory auditors provide independent reasonable assurance on individual and consolidated financial statements, thereby enhancing users' (investors, creditors, depositors, policyholders and supervisors) confidence in the accuracy and integrity of financial reports. For issuers in regulated markets, audit assurance is embedded in the EU disclosure framework[4]. This assurance function is integral to market transparency, investor protection and orderly functioning of the EU's primary and secondary markets.

15) Auditors' ability to perform their mandate depends critically on maintaining the confidentiality, integrity and availability of the information obtained from their clients throughout the audit process and after its completion. The audit process involves the acquisition and analysis of auditee's data, which may, depending on sensitivity, be accessed directly on systems controlled by the auditee or transferred externally. Any compromise to this information may undermine the reliability of the audit, damage the reputation of the auditee and weaken the confidence of supervisors, investors and markets in the audited financial statements. It may also affect the reputation of the auditors themselves, therefore their ability to maintain their operation and attract new business and, finally, increase market concentration. Such a disruption may have significant financial and reputational implications for the auditee. Indeed, the audit review is critical for issuers to discharge their legal responsibilities under the Transparency Directive and other relevant sectoral legislations, when applicable, and any failures could have regulatory consequences for the issuers (including breaches of covenants) and potentially on the financial stability. However, most of time, it would not directly affect the continuity of the auditee's operational services. Indeed, the audit function, although essential for trust and market confidence, is typically not embedded in the day-to-day operational value chain of the audited entity and therefore is not critical for the continuous provisioning of financial (or other) services to clients from an operational perspective.

16) The Statutory Audit Directive and Regulation (EU) No 537/2014 establish organisational requirements relevant to the digital operational resilience of the statutory auditors and the audit firms, though such provisions are quite high-level and limited given the importance of auditors in charge of public-interest entities for the financial entities:

    a. Article 24a(1) of Directive 2006/43/EC requires, among other things, statutory auditors and audit firms to: (1) use appropriate systems, resources and procedures to ensure continuity and regularity in the carrying out the statutory audit activities; (2) establish [...] arrangements for dealing with and recording incidents which have, or may have, serious consequences for the integrity of statutory audit activities.

[4] For listed issuers, statutory audit forms an integral part of EU market disclosure obligations. The Transparency Directive (Directive 2004/109/EC, Article 4) requires issuers on regulated markets to publish audited annual financial statements and the corresponding audit report. For securities offerings and admissions to trading, Regulation (EU) 2017/1129 and Commission Delegated Regulation (EU) 2019/980 (Annex 1) require audited historical financial information to be included in the prospectus

b. Article 15 of Regulation (EU) No 537/2014 requires statutory auditors to have five-year minimum record-retention for all audit documentation.

17) At operational level, audit engagements are governed by contractual arrangements between auditor and auditee specifying secure means of data exchange (e.g. encrypted portals, virtual data rooms, and confidentiality clauses). Furthermore, in some instances, auditors and auditees have developed infrastructures (e.g. interfaces) used on an ongoing basis which should be properly managed. It is also noted that auditors and statutory auditors must comply with all applicable cross-sectoral data-protection regulations (e.g. the General Data Protection Regulation), which collectively strengthen the safeguards in place to ensure the security of data.

18) While the references to ICT resilience in EU audit law are general, auditors already operate within a multi-layered framework—comprising both regulatory requirements and contractual safeguards—that may contribute to the protection of information and support their digital resilience.

19) Furthermore, as statutory auditors and audit firms provide their services to– among other clients - financial entities, and the financial entities must implement the relevant ICT risk mitigation measures complying with DORA, in case the auditors directly access the systems of their clients, the mitigation measures (such as access control) should also impact the auditors in the delivery of the audit services. Other measures, may relate to the use of data rooms and encrypted portals or datasets.

Potential implications of extending the scope of DORA to statutory auditors and audit firms

20) While confidentiality, integrity and availability of audit information are crucial, extending DORA to statutory auditors and audit firms would have several significant implications:

a. Market perspective. Empirical evidence (e.g. CEAOB/Commission Joint Reports[5]) confirm that the EU audit market is highly concentrated, with the largest firms ("Big Four") auditing the vast majority of public-interest entities. Applying all DORA requirements could increase fixed compliance costs, thereby reinforcing concentration by making market entry or survival harder for mid-tier and smaller audit firms. This could reduce audit choice for the auditees, not in line with the objective of fostering competition and audit quality as pursued by Regulation (EU) No 537/2014, and with the administrative burden reduction target of the European Commission.

b. Auditees perspective (not only financial entities). Provided the ICT operational resilience requirements applicable for auditors are different from the DORA requirements, extending DORA as a whole to audit firms could increase audit fees, as firms would face additional compliance and ICT investment costs. In the case of mid-tier and smaller auditors, such increasing costs might not be neutral on their audit fees to be paid by their clients and might have a tangible impact on some of them (e.g small and medium-sized enterprises or the microenterprises). The added value of DORA-compliant auditors may not outweigh the higher audit fees they incur.

[5] See for information: EUR-Lex - 52024DC0102 - EN - EUR-Lex

c. Supervisory perspective. The inclusion of this type of entities in the scope of DORA would likely require an important effort in re-skilling the workforce of the national competent authorities in charge of the supervision of the statutory auditors and audit firms as they would need to deal with: (i) reporting of ICT-related incidents; (ii) maintenance of ICT risk registers; (iii) participation in TLPT testing where required; and (iv) general DORA compliance supervision.

d. Implementation & governance perspective. To include auditors of public-interest entities in the scope of the entities subject to the DORA framework would have several side effects and interplays, with impacts on the financial sector and its relevant authorities. The ESAs can at least identify the following:

- ICT-related incident management framework (DORA Chapter III): As part of the requirements related to the ICT-related incident management, classification and reporting, competent authorities in charge of the entities subject to DORA shall notify the ESAs and other EU and national authorities once they are notified by financial entities of major ICT-incidents. While the ESAs shall report yearly on major ICT-related incidents, the inclusion of the auditors in the scope of DORA would necessitate clarifications regarding the impact on the ESAs' mandates towards major incidents notifications sent by the auditors (collection, dissemination). On the same vein, the ESAs' Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents (based on article 11(11)), might need to be amended if the ESAs would have new responsibilities towards auditors' major incidents.

- Threat-Led Penetration testing / TLPT (DORA Chapter IV): Article 26(9) and (10) allow the Member States to designate a single national public authority in the financial sector to be responsible for TLPT-related matters. In case the statutory auditors and the audit firms would be subject to TLPT requirements as well, a new kind of authority (not from the financial sector) might be considered for the appointment of such national TLPT-authority, involving unanticipated new coordination needs.

- DORA Oversight framework (DORA Chapter V, Section II): The DORA Oversight Framework involves many EU and national competent authorities of the financial sector (or NIS authorities), at various levels, and grants them new responsibilities. The inclusion of auditors in this framework would have several important consequences. First, the auditors would have to contribute to the data collection of the Register of Information, and their competent authorities would have to collect all the registers for the ESAs and the CEAOB to feed the overall CTPP designation process. Second, national competent authorities of auditors would be required to join the Oversight Forum and the technical fora where IT implementation is discussed; and they would also have to involve staff within the Joint Examination Teams (JETs) like the CAs of the financial entities. The involvement in the JETs has to be properly anticipated, and the current experience of the ESAs and the CAs implementing the oversight framework evidence that the impact on the resources is significant: authorities often have to recruit additional staff to

compose the oversight teams. Third, as the CEAOB has no legal authority, no budget and no proper resources, clarifications should be provided on which authority could be appointed as Lead Overseer in case a CTPP would be designated because it would be foremost critical for the auditors of public-interest entities (based on article 31(1)(b)). The appointment as Lead Overseer implies important organisational arrangements and responsibilities for the appointed authority. Fourth, as the DORA Oversight Framework is built to support and complement the capabilities of the authorities supervising the entities using the CTPPs, national competent authorities of auditors would have to follow-up with the auditors subject to DORA to ensure that they take the relevant measures considering the risk identified by the oversight teams.

- Cooperation between authorities (DORA Chapter VII): Articles 47 to 49 indicate that competent authorities involved in the implementation of the DORA framework have to cooperate. When those authorities are not part of the ESAs Board of Supervisors, the implications related to decision-making model of the ESAs in relation to DORA may need to be further assessed, as well as their potential involvement in the NIS Cooperation Group, the existing CSIRTs networks, and the European Systemic Cyber Incident Coordination Framework (EU-SCICF).

e. Inclusion of service providers in the scope of DORA : The use by financial entities of statutory auditors and audit firms to certify their financial statements is mandatory, unlike most other service providers. However, financial entities also rely on several non-regulated providers (e.g., ICT service providers, legal and tax advisors, HR and facility management, crisis communication, energy suppliers). Those providers may have access to sensitive information or be essential to their operations, without being subject to DORA. For instance, even ICT third-party service providers under DORA are not subject to most of the requirements applicable to the financial entities, even though they are essential for the delivery of the financial services. Extending DORA to statutory auditors does not appear more justified than extending it to these other providers, given that DORA is specifically tailored to the financial sector.

Conclusion and recommendation

21) The ESAs recognise the crucial public-interest role of statutory auditors, certifying the financial statements of the public-interest entities, including also the financial entities. In order to carry out their statutory tasks, auditors need to access auditees data, which need to be properly protected by measures defined both by the Auditee and the Auditors. The oversight of audit firms lies primarily with the national audit oversight authorities and the CEAOB under Directive 2006/43/EC and Regulation 537/2014. While the ESAs acknowledge that the current regulatory framework applicable to statutory auditors and audit firms include only high-level, indirect and limited reference to digital operational resilience, the identified implications of the application of DORA to the statutory auditors and audit firms appear to outweigh the potential benefits. The ESAs therefore consider that including statutory auditors and audit firms within DORA's scope is not warranted at this stage.