European Banking Authority

PEER REVIEW FOLLOW-UP REPORT ON ICT RISK ASSESSMENT UNDER THE SREP

EBA/REP/2026/05 FEBRUARY 2026

Table of Contents

Abbreviations

CA	Competent Authority
CRD	Capital Requirements Directive (Directive 2013/36/EU)
CRR	Capital Requirements Regulation (Regulation (EU) No 575/2013)
DORA	Digital Operational Resilience Act (Regulation (EU) 2022/2554)
EBA	European Banking Authority
ICT	Information and Communication Technology
ICT SREP guidelines	Guidelines on the ICT risk assessment under the Supervisory Review and Evaluation Process (SREP)
MS	Member State
PRC	Peer Review Committee
SREP guidelines	Guidelines for common procedures and methodologies for the Supervisory Review and Evaluation Process (SREP) and supervisory stress testing
TLPT	Threat-Led Penetration Testing

Executive Summary

This report is a follow-up to the EBA 2022 peer review report on the ICT risk assessment under the SREP[1], developed in accordance with Article 11 of the methodology for the conduct of peer reviews[2]. It assesses the progress made by prudential supervisors in implementing the recommendations from the 2022 peer review report.

This report follows significant regulatory developments, notably the Digital Operational Resilience Act (DORA)[3] which applied from January 2025 and fundamentally reshapes ICT risk supervision across the EU financial sector. Moreover, following a recommendation of the 2022 Report, ICT risk assessment is being incorporated into the revised guidelines on the supervisory review and evaluation process (SREP) which will replace the standalone ICT SREP guidelines.

These changes and substantial implementation efforts made by supervisors and financial institutions have significantly shaped the approach to this follow up report, which largely used existing EBA supervisory convergence work to carry out the assessment of how supervisors have implemented the recommendations of the original peer review.

Notable improvements were found with regard to those recommendations. Supervisors are in the process of strengthening their ICT supervisory capacity and expertise, progressing with the use of horizontal analysis and the systematic use of supervisory tools. Furthermore, some improvement was noted in relation to the benchmarks on the use of the list of ICT risk sub-categories and risk scenarios with a number of supervisors now having these in place, although with few gaps still remaining. Regarding the development of a dedicated methodology for ICT risk assessment, there has been no overall change as with one exception all CAs have established such a methodology.

Continued investment and efforts in ICT expertise, horizontal analysis, and supervisory tools will be critical to ensure effective ICT risk supervision under DORA and the revised SREP guidelines.

[1] Peer Review Report on ICT Risk assessment under the SREP.pdf
[2] EBA Methodology for the conduct of peer reviews (EBA/DC/2020/327)
[3] Regulation (EU) 2022/2554 https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

1. Introduction

1.1. Background

1. This report is a follow-up to the EBA peer review on the ICT risk assessment under the SREP (EBA/REP/2022/25) which was conducted in 2021 – 2022, the findings of which were published on 17 October 2022 (the "2022 Report"). The 2022 Report found that competent authorities ("CAs") across the EU had largely implemented the EBA Guidelines on ICT risk assessment under the SREP ("ICT SREP guidelines") and had applied them in their supervisory practices. Moreover, a series of recommendations were set out along with CAs' responses to several benchmarking questions.

2. In line with Article 11 of the EBA Peer Review Methodology[4], two years after the publication of a peer review report, the EBA publishes a follow-up report, which includes "an assessment of, but not be limited to, the adequacy and effectiveness of the actions undertaken by the competent authorities that are subject to the peer review in response to the follow-up measures of the peer review report".

3. Since the publication of the 2022 Report, significant regulatory changes have taken place, most importantly the entry into force of DORA in January 2023 and its entry into application in January 2025. Moreover, as a result of the introduction of DORA and the related recommendation set out in the 2022 Report, the ICT SREP guidelines will be repealed and integrated into the upcoming revised SREP guidelines to ensure consistency and foster simplification. An explanation of the related regulatory changes is set out in Chapter 2.

4. The 2022 Report also found that one CA had yet to set up a dedicated methodology for ICT risk assessment and a few CAs had yet to use the list of ICT risk sub-categories and risk scenarios set out in the Annex of the ICT SREP guidelines. A series of recommendations were addressed to all the CAs in the 2022 Report as follows:
   - CAs should build up the necessary capacity and expertise, which is key to effective supervision in ICT risk assessment.
   - CAs which do not perform horizontal analysis should begin doing so, in particular to detect outliers and also to ensure a level playing field.
   - In order to allow for a proportionate approach to ICT risk assessment, CAs should make use of available tools such as self-assessment questionnaires, IT landscape analyses and to support the supervisory work with automated tools where available.

5. The 2022 Report also set out several recommendations addressed to the EBA. These recommendations are being reflected in the upcoming revised SREP guidelines, specifically the

[4] EBA Methodology for the conduct of peer reviews (EBA/DC/2020/327)

enhanced focus on ICT risk assessment by incorporating the DORA framework and incorporation of the existing ICT SREP guidelines which will then be repealed.

1.2 Methodology

6. The follow-up peer review was performed by a Peer Review Committee (PRC) comprised of EBA and CA staff (see Annex 1 for the composition). The follow-up peer review focuses on the recommendations to the CAs and targeted benchmarking questions covered in the 2022 Report.

7. The approach to this report takes into account the ongoing implementation efforts on DORA and the upcoming revised SREP GL. To that end a pragmatic approach was taken for this follow-up peer review, and therefore the follow-up of the recommendations to the CAs was assessed using information provided by CAs since 2022 through ongoing EBA supervisory convergence activities and monitoring tools.

8. The PRC concentrated on some benchmarking aspects from the 2022 Report as few CAs were found to have developed a dedicated methodology for ICT risk assessment or developed a list of ICT risk sub-categories. The follow-up of the benchmarking was carried out through a dedicated set of questions sent to each CA that reported 'no' or 'not yet, but planning' in questions 2 and 20 of the 2022 Report.

9. The significant regulatory changes taking place at the time of drafting this report are outlined in the section below and they have substantially shaped the approach taken for this follow-up. Given the regulatory changes which are afoot, it is the view of the PRC that monitoring activities should continue in the area of ICT risk. This is also warranted by the evolving methodological context regarding ICT supervision and the increasing emphasis on ICT risk assessment, likely impacting resource allocation and capacity requirements.

2. Regulatory Changes

10. This section provides an overview of the significant regulatory changes that have taken place since the 2022 Report and have triggered the review of the ICT-related methodologies and supervisory practices, which are now undergoing substantial updates and are being integrated into a more robust and unified EU framework.

a) Shortly after the publication of the 2022 Report, the DORA entered into force in January 2023 and entered into application in January 2025. DORA establishes a unified and directly applicable framework for digital operational resilience across the EU financial sector, with comprehensive requirements for financial entities regarding the management of ICT risk. DORA covers key components of ICT risk management with harmonised requirements on:

- *ICT risk management*: Regarding the implementation of robust governance, risk management, and control frameworks for ICT, covering identification, protection, detection, response, and recovery.
- *Incident reporting*: Regarding the classification and reporting of major ICT-related incidents, enabling timely supervisory intervention and sector-wide situational awareness.
- *Digital operational resilience testing*: Regarding the conduct of regular and advanced testing of financial entities' ICT systems, including threat-led penetration testing for certain financial entities.
- *ICT third-party risk management*: Regarding the sound management of ICT third-party risk. DORA also establishes a new oversight regime for critical ICT third-party service providers.

Several technical standards and guidelines have been developed to supplement DORA, providing further specifications to both the CAs and financial entities for its effective and consistent implementation. In particular, the Commission Delegated Regulation (EU) 2024/1774[5] further specifies ICT risk management tools, methods, processes, and policies transformed previously recommended or unevenly applied practices into binding, directly applicable requirements, ensuring that all EU financial entities adhere to a unified and robust ICT risk management regime. This marks a fundamental change of the landscape assessed in the 2022 Report, as a uniform baseline has been now set to promote a level playing field and enhance supervisory effectiveness and resilience within the EU financial sector.

b) The introduction of the DORA framework and the 2022 Report recommendation to the EBA to incorporate the ICT SREP guidelines into the general SREP guidelines were among the key

[5] Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework

drivers for the revision of the general SREP guidelines[6] . This revision will lead to the repeal of the ICT SREP guidelines, and it will integrate the ICT risk assessment into the operational risk assessment (Title 6 of the upcoming revised SREP guidelines). The upcoming revised SREP guidelines will integrate the DORA framework and reflect changes stemming from CRD IV/CRR III[7], ensuring ICT risk is fully embedded in the supervisory framework and explicitly included within operational risk. When it comes to ICT aspects, the upcoming revised SREP guidelines will place more emphasis on third-party risk management and governance aspects of ICT risk management, enhancing proportionality with ICT risk being assessed in the same consolidated SREP process, rather than in parallel tracks, and following the minimum SREP engagement model. Furthermore, the upcoming revised SREP guidelines will specify that when assessing operational risk, CAs should assess ICT risk pursuant to the DORA framework and its potential impact on the institution's critical or important functions, including any potential financial, reputational, regulatory and strategic impact. Lastly, the upcoming revised SREP guidelines will foresee the integration of institution-specific DORA-related indicators into the CAs' monitoring frameworks.

11. The significant regulatory changes were reflected in the annual supervisory priorities[8] set by the EBA, taking into account the findings of the 2022 Report: elevating ICT risk and digital resilience to a priority, aligning with DORA, and strengthening ICT risk supervision. In doing so, the supervisory priorities served as the forward-looking framework by which the 2022 Report recommendations were operationalised. Moreover, across the EBA's supervisory priorities, the focus on ICT risk has primarily focused on the implementation of DORA. This reflects the ongoing implementation efforts towards a harmonised and comprehensive regulatory and supervisory framework on ICT risk, established under DORA.

12. Moreover, the EBA is publishing a report each year on the degree of convergence of the SREP, which also provides the annual monitoring observations from which the various peer review recommendations can be assessed. The annual EBA supervisory priorities and convergence work support this follow-up and help embed the peer review's findings into forward supervisory action.

[6] https://www.eba.europa.eu/publications-and-media/press-releases/eba-consults-revised-guidelines-supervisory-review-and-evaluation-process-and-supervisory-stress

[7] For further information, please refer to the CP of the revised SREP GL.

[8] The EBA sets on an annual basis key topics for heightened supervisory attention to fulfil its mandate in driving convergence in supervisory practices across the EU.

3. Follow-up of recommendations and benchmarking

3.1. Follow-up of peer review recommendations to CAs

13. To monitor the follow-up on the recommendations provided to CAs in the 2022 Report various sources of information have been considered, including the annual EBA supervisory convergence reports and supervisory priorities (European Supervisory Examination Programmes), annual EBA work programmes, peer review on the application of proportionality under the SREP[9], supervisory exchanges and other relevant activities.

14. Since the introduction of DORA, supervisory priorities increasingly emphasise ICT risk management, operational resilience, and readiness for the DORA. They have been raising the supervisory profile of ICT-related issues, promoted convergence of supervisory focus on ICT-related aspects and fostering the development of supervisory capacity for digital operational resilience and alignment with DORA. Across the EBA supervisory convergence work, sustained supervisory focus on ICT risk and operational resilience has been reported, with CAs applying the EBA ICT-related supervisory priorities since 2022. While certain areas are undergoing improvement (e.g. resourcing and specialised ICT skills), the ongoing EBA supervisory activities provide strong evidence of implementation of the 2022 Report recommendations.

3.1.1. Build up ICT-related capacity and expertise

15. The **first recommendation** to the CAs was the building up of the necessary capacity and expertise which is key to effective ICT risk supervision. The importance of keeping the required skillset up to date was noted in view of the changing ICT and regulatory landscape, for example in light of the DORA. Training curriculums on ICT risk were proposed to be developed where not yet available. These could be supplemented with other initiatives to enhance the expertise of ICT experts and build up the knowledge of general supervisors in ICT risk such as the use of forums to share and enhance expertise, horizontal ICT risk expert networks, mentoring by ICT experts, and the involvement of general supervisors in ICT related work.

16. Throughout its monitoring activities, the EBA collected information on the CAs' ongoing efforts to prepare for their supervisory responsibilities under DORA and to enhance their ICT-related capacity and expertise. CAs have been setting up or enhancing dedicated ICT teams/roles or DORA-specific supervisory units to prepare for their new responsibilities under DORA. Where such teams or units already exist, CAs have been reinforcing them by recruiting or adding ICT specialists (e.g. on threat-led penetration testing) to strengthen ICT supervision. In addition,

[9] https://www.eba.europa.eu/publications-and-media/press-releases/eba-publishes-its-peer-review-application-proportionality-under-supervisory-review-and-evaluation

targeted training programs have been delivered by CAs to enhance technology/cyber-related skills, including among generalist staff profiles, further supporting the overall supervisory capacity. It is also worth noting that CAs provided a series of awareness/information sessions, workshops and seminars/webinars to supervised institutions to introduce DORA and to enhance focus on ICT risk.

17. Furthermore, to enable the coordination envisaged in the DORA framework and to strengthen their ICT expertise, CAs established or enhanced cooperation with other relevant authorities (for example national competent authorities for the NIS Directive[10]), including the conclusion of Memoranda of Understanding, and participated in EU-wide workstreams on the DORA implementation.

18. To support building ICT-related capacity and expertise, the EU Supervisory Digital Finance Academy (EU-SDFA) was established in 2022 by the European Commission in cooperation with the ESAs. This initiative aims at supporting supervisory authorities in coping with the risks and opportunities stemming from use of advanced technologies in the financial sector. The EU-SDFA encompasses comprehensive training cycles and workshops enabling the acquisition of new expertise and skills, knowledge sharing and peer-to-peer exchanges within the supervisory community. To date, more than 2000 supervisors were trained from 44 national competent authorities (covering 27 MS) and training sessions included ICT-related topics such as DORA introduction, ICT risk management, ICT incident management, ICT third-party risk management, cybersecurity risk. These activities aim to strengthen supervisory capacity, to support supervisory convergence and to bridge technology, regulatory and supervisory knowledge.

19. In addition, the EBA develops a training programme[11] for staff of CAs based on the EBA's work programme and the specific needs expressed by CAs such ICT-related skills[12]. These offerings include seminars, online courses and collaborative workshops, often hosted on the EBA Learning Hub, and are designed to strengthen supervisory skills, promote best practices and support the implementation of the single rulebook.

20. This recommendation is, by nature, an ongoing process, as also reflected in the EBA's annual supervisory convergence reports, which consistently highlight training and capacity building as key follow-up tools. Significant progress has been achieved in ICT risk supervision, particularly driven by DORA, with many authorities strengthening their ICT capabilities. Nevertheless, further efforts remain necessary to fully meet the objectives and ensure sustained capacity building over time. These could focus on enhanced training and skill development (e.g. ICT risk training curriculums and regulated training sessions), expertise enhancement initiatives (e.g.

[10] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[11] www.eba.europa.eu/sites/default/files/2025-09/87f724cd-ff01-4415-9a23-e06cee3daec7/EBA%20Course%20Offer%20for%20externals%20-%20August%202025%20Edition%20-%20for%20website.pdf

[12] Indicatively, the Autumn 2025 EBA course offer included webinar on ICT and security risk management, online course on cloud computing, workshops on SupTech adoption and AI.

ICT risk expert networks, mentoring programmes, cross-authorities collaboration), broader involvement of general supervisors (e.g. participation of general supervisors in ICT-related supervisory work, cross-functional projects) and continuous improvement (e.g. use of KPIs/metrics, feedback loop, annual review of ICT risk supervision capacity).

3.1.2. Horizontal analysis

21. The **second recommendation** to the CAs, which did not perform horizontal analysis as part of their supervision of ICT risk, was to set up this comparison, in particular for detecting outliers, and assuring a level playing field in their jurisdiction. In addition, thematic horizontal analyses were proposed in specific ICT risk areas based on a risk-based approach and according to supervisory priorities. The use of horizontal analyses was particularly useful for CAs in charge of supervising a large number of smaller and less complex institutions. The analyses can assist in flagging potential weaknesses in individual institutions or areas of supervisory concern among institutions based on which the CAs can plan further supervisory work in these specific areas.

22. Through its monitoring activities, the EBA collected information on the CAs' ongoing efforts to enhance ICT-related horizontal analyses, which is significantly promoted through the DORA framework and the upcoming revised SREP guidelines. With the introduction of DORA, CAs performed sector-wide surveys to assess the level of DORA implementation (e.g. risk-based/multiple-step surveys, self-assessment questionnaires), initiated horizontal benchmarking and designed risk-based supervisory activities reflecting supervisory priorities.

23. Horizontal analysis is increasingly integrated into ICT risk supervision mainly due to DORA, as CAs have been preparing for ICT-related incident reporting exercises, and thematic/horizontal reviews, including on-site inspections (for example on third-party risk management and incident handling) which were reinforced in 2025, while more in-depth horizontal activities are planned from 2026 onwards. In 2025, the first annual collection and aggregation of registers of information on ICT services contracted to ICT third-party providers was performed by all the CAs covering all the EU credit institutions, aiming to enhance ICT third-party risk monitoring by credit institutions and to allow CAs to obtain a horizontal overview of the ICT services. In addition, ICT-related incidents have been reported by the supervised institutions to the CAs and these have been used (among others) to identify systemic patterns and recurring vulnerabilities across supervised institutions (horizontal analysis) and to benchmark ICT risk management and incident response capabilities of individual institutions against peers. CAs have automated or are in the process of automating these data collections for efficiency and broader coverage purposes.

24. Furthermore, the EBA supervisory convergence report[13] (2022) noted that CAs used several different tools such as specific FinTech and/or ICT SREP/risk assessment questionnaires,

13 https://www.eba.europa.eu/sites/default/files/document_library/Publications/Reports/2023/1055271/Report%20on%20convergence%20of%20supervisory%20practices%20in%202022.pdf

horizontal analysis and benchmarking, on-site activities, and off-site monitoring to supervise the implementation of the digital transformation and review institutions' approach towards FinTech solutions. CAs also noted the establishment of a database from their findings which could facilitate their horizontal analysis.

25. It should be also noted the peer review on the application of proportionality in the SREP[14] identified several best practices allowing for the efficient use of supervisory resources in the application of proportionality, also applicable to ICT risk assessment, including the conduct of thematic SREP assessments on multiple institutions as a single assessment ('clustering'), the use of benchmarking tools, 'pilot inspections' where several institutions use the same service provider, and spot checks on the quality, accuracy and reliability of information provided by institutions in self-assessment questionnaires.

26. Complementary to the above, under the upcoming revised SREP guidelines, CAs will need to consider minimum key ICT-related risk factors (e.g. ICT operations, ICT systems, third-party arrangements) and to benchmark the institution's position against its peers for the assessment of inherent operational risk.

27. To date, noticeable progress has been made by CAs to conduct horizontal and thematic analyses on ICT risks, supported by the DORA framework. However, full maturity is yet to be achieved as CAs continue to expand automation and embed horizontal analysis into the supervisory frameworks.

3.1.3. Use of available tools

28. The **third recommendation** to the CAs was the use of available tools such as self-assessment questionnaires, IT landscape analyses, automated tools where available to support the supervisory work. This aimed to allow for a proportionate approach to the ICT risk assessment under the SREP and in particular to facilitate and enhance the effectiveness and efficiency of their work.

29. Throughout its monitoring activities, the EBA collected information on the CAs' ongoing efforts to enhance the use of available tools for ICT risk supervision, and in particular under DORA, which has prompted CAs to leverage on certain tools more systematically and integrate them into their supervisory practices.

30. With the introduction of DORA, a widespread use of self-assessment surveys and questionnaires by CAs to assess DORA readiness and ICT risk maturity was noted. CAs have implemented or are developing automated systems for incident reporting and collection of registers of information, including the use of online platforms to facilitate submission and analysis. Some CAs have developed targeted tools and automated data collection platforms while others have upgraded existing platforms for incident and cyber threat reporting, and are

[14] https://www.eba.europa.eu/publications-and-media/press-releases/eba-publishes-its-peer-review-application-proportionality-under-supervisory-review-and-evaluation

actively aligning their processes with DORA, NIS2, and other EU regulations. Automated validation engines and support systems are also in use to enhance data quality and compliance. Another example is the use of an AI tool by a CA (NL) for assessing DORA compliance of contracts with third-party providers.

31. Notably, the 2022 supervisory convergence report noted that CAs used a wide range of supervisory tools, such as ICT risk assessment questionnaires as part of SREP, review and analysis of incident registry, review of continuity plans for critical outsourced activities, on-site thematic inspections on service providers and off-site monitoring. The interactions with the supervised institutions included but not limited to interviews with ICT-security managers, meetings with top management and internal control functions, correspondence and information exchange using secure channels.

32. Similarly to the previous recommendations, the use of available supervisory tools is, by nature, an ongoing process, as their effective use requires continuous adaptation and refinement. While strong progress has been noted, particularly under DORA, ongoing efforts are expected to continue ensuring these tools are used consistently and to their full potential. Indicatively, these could focus on comprehensive use of ICT risk landscape analysis tools and integration of automated tools into supervisory workflows, along with training on their effective use to supervisors.

3.2. Follow-up of benchmarking

33. To assess the follow-up of the benchmarking a dedicated set of questions was sent to each CA that reported '*no*' or '*not yet, but planning*' relating to benchmark question 2 (the setting up of a dedicated methodology for ICT risk assessment) and benchmark question 20 (the development of a list of ICT risk scenarios and sub categories) of the 2022 Report. It should be noted that the follow-up of benchmarking question 5 (set up of a methodology to assign an ICT risk score) was deemed to provide limited added value in light of the upcoming revised SREP guidelines. Specifically, rather than prescribing the operational risk sub-categories to be scored individually (under the risks to capital), the upcoming revised SREP guidelines will allow CAs to score risk sub-categories individually depending on the materiality of these risk sub-categories to a particular institution. This will apply to ICT risk (as a risk sub-category of operational risk) and the upcoming revised SREP guidelines will clarify that CAs should always pay attention and assess ICT risk, pursuant to the DORA framework.

3.2.1. Dedicated methodology for ICT risk assessment

34. The 2022 Report revealed that with one exception, all the CAs have set up a dedicated methodology for ICT risk assessment (at least partially for 8 among 31 authorities). The PRC followed up with the one CA (HU) which noted that its SREP assessment methodology remains unchanged, with an update planned in the near future to align with DORA, hence it remains non-compliant in this respect.

35. It is further noted that according to the EBA monitoring activities, the CAs have updated their supervisory manuals, methodologies, and internal procedures to reflect and align with DORA requirements and evolving ICT risks. Some are still in progress, especially where national legislation is being finalised.

3.2.2. List of ICT risk sub-categories and risk scenarios used

36. The 2022 Report revealed that most CAs applied the list of ICT risk sub-categories and risk scenarios set out in the Annex of the ICT SREP guidelines. The PRC followed up with the four CAs (BG, FR, LI, SE) which did not apply that list to assess the implementation of benchmarking question 20. One CA (FR) fully uses and two CAs (SE and LI) broadly use the list of ICT risk sub-categories, while BG still does not and only plans to do so from 2026 remaining non-compliant in this respect at the time.

4. Conclusions

37. The follow-up peer review demonstrates notable improvement from the side of the CAs on the implementation of the recommendations of the 2022 Report and their overall approach to ICT risk supervision. The DORA adoption and the forthcoming integration of ICT risk into the revised SREP Guidelines are fundamentally reshaping the supervisory landscape, establishing a harmonized and robust framework for ICT risk management across the EU.

38. Overall, CAs are in the process of strengthening their supervisory capacity and expertise, notably through the creation of dedicated ICT teams, targeted training programs, and participation in EU-wide initiatives. These efforts have enhanced readiness for DORA implementation and improved convergence in supervisory practices. Nevertheless, capacity building remains an ongoing priority, particularly in light of evolving technological and regulatory challenges.

39. Progress has also been observed in the use of horizontal analysis and benchmarking, which are increasingly embedded in supervisory approaches. Sector-wide surveys, thematic reviews, and incident reporting exercises have enabled CAs to identify systemic vulnerabilities and promote a level playing field. While these practices are not yet fully mature, their expansion under DORA and the revised SREP guidelines is expected to further strengthen supervisory effectiveness.

40. The use of supervisory tools—such as self-assessment questionnaires, automated data collection platforms, and incident reporting systems—has become more systematic and technologically advanced. These tools support proportionality, efficiency, and consistency in ICT risk supervision, aligning with the objectives of DORA and the upcoming SREP framework.

41. Despite these achievements, some areas of improvement remain, particularly regarding the full integration of ICT risk methodologies and ICT risk sub-categories into supervisory manuals and processes. These are expected to be addressed as CAs finalise their alignment with DORA and the revised SREP guidelines. Given the dynamic nature of ICT risks and the evolving regulatory environment, continued efforts will be essential to maintain supervisory convergence and operational resilience. CAs that have not yet applied the benchmarks are encouraged to enhance their practices to align more closely with the other CAs in the area.

42. The follow-up review demonstrates strong progress in implementing the 2022 recommendations and adapting to the new regulatory framework. However, sustained investment in expertise, horizontal analysis, and supervisory tools will be critical to ensure effective ICT risk supervision under DORA and the revised SREP guidelines. To this end, the findings of the follow-up report do not necessitate any further recommendations on the topic. A future peer review may be warranted to assess the maturity of these developments or the implementation of a targeted ICT area.

Annex 1. Peer Review Committee

Peer reviews are carried out by ad hoc peer review committees composed of staff from the EBA and members of competent authorities, and chaired by the EBA staff.

This peer review was carried out by:

Co-chairs
Jonathan Overett Somnier
Head of Legal and Compliance Unit, EBA

Andreas Papaetis
Senior Policy Expert, Prudential Regulation and Supervisory Policy (PRSP), EBA

Members
Adrienne Coleton
Legal Expert, Legal and Compliance Unit, EBA

José Gabriel Criado Giménez
IT Audit Expert, Dirección General de Supervisión, Banco de España

Efthymios Papanikolaou
Team Lead, Oversight of Third-Party Providers, Directorate General Horizontal Line Supervision, European Central Bank

Salvatore Vitiello
Advisor, Directorate General for Financial Supervision and Regulation, Banca d'Italia

Tour Europlaza, 20 avenue André Prothin CS 30154
92927 Paris La Défense CEDEX, FRANCE
Tel. +33 1 86 52 70 00

E-mail: info@eba.europa.eu

https://eba.europa.eu