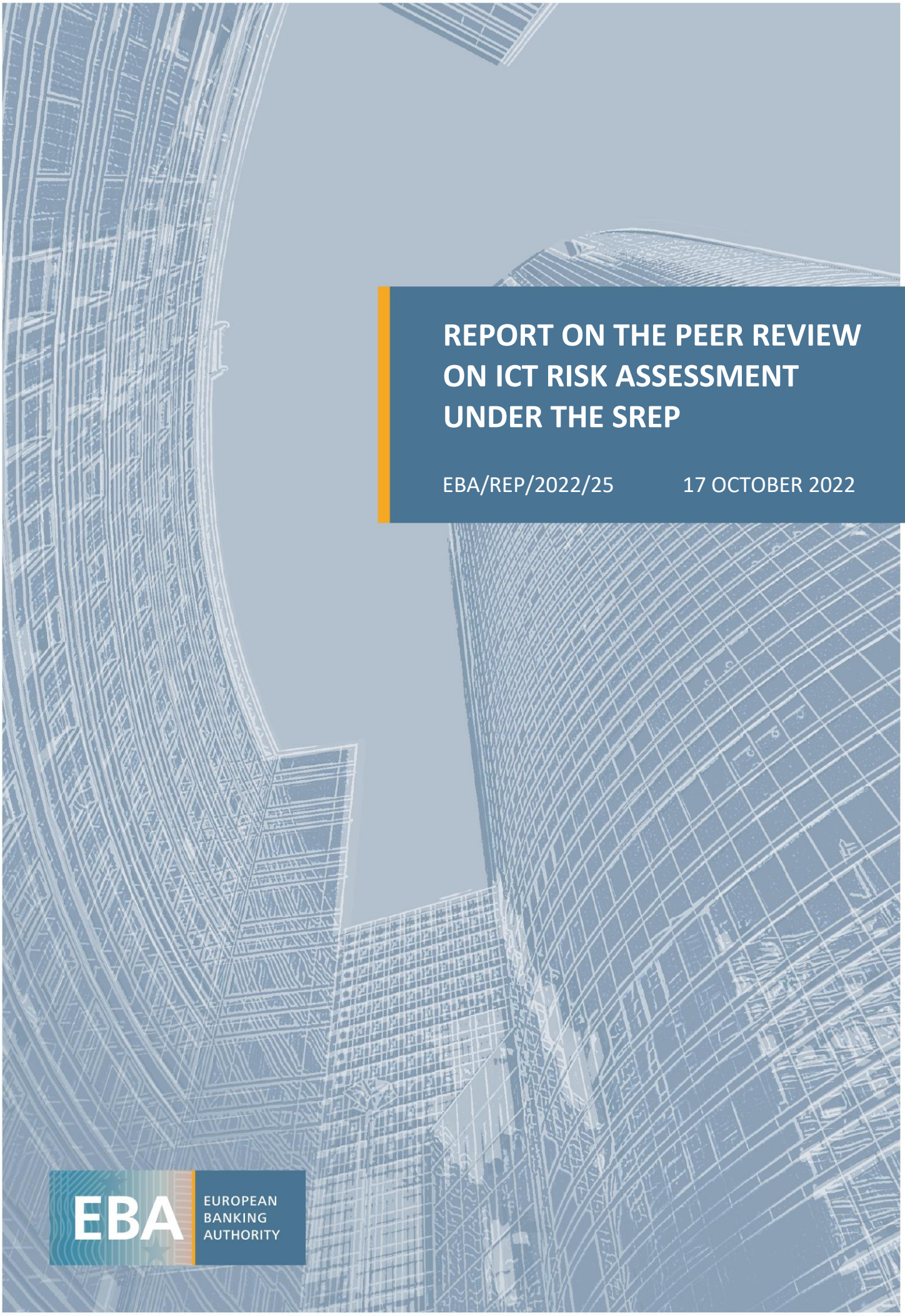


REPORT ON THE PEER REVIEW ON ICT RISK ASSESSMENT UNDER THE SREP

EBA/REP/2022/25 17 OCTOBER 2022

EBA EUROPEAN BANKING AUTHORITY

Contents

List of abbreviations 3

Executive Summary 4

1. Background and rationale 6

1.1 Introduction 6

1.2 EBA Guidelines on ICT Risk Assessment under the SREP 6

1.3 Competent Authorities notification of Comply or explain 7

1.4 Scope and methodology 7

2. Peer review outcomes and recommendations 9

2.1 Summary of findings 9

2.1.1 General implementation of the Guidelines 9
2.1.2 Challenges faced in the assessment of ICT risks 10
2.1.3 Supervisory practices in ICT risk assessment under the SREP 10

2.2 Good practices developed by competent authorities 11

2.3 PRC recommendations 13

2.3.1 Recommendations to CAs 13
2.3.2 Recommendations to the EBA 13

3. Assessment of practices of competent authorities 15

3.1 Implementation of the EBA Guidelines on ICT Risk assessment under the SREP 15

3.1.1 General implementation 15
3.1.2 Proportionality 15
3.1.3 Incorporating the assessment of ICT risks in the SREP 16
3.1.4 Assessing ICT risks in the SREP as a sub-category of operational risk 16
3.1.5 ICT risks in the score for operational risk 16
3.1.6 Inputs used in the assessment of ICT risks 17
3.1.7 Challenges faced in the assessment of ICT risks 17
3.1.8 Horizontal analysis in the assessment of ICT risks 18

3.2 Supervisory practices in the ICT risk assessment under the SREP 18

3.2.1 General supervision, prioritization and resources 18
3.2.2 Assessment of ICT risk 20
3.2.3 Assessment of materiality of ICT risk and ICT risk taxonomy 20
3.2.4 Assessment of ICT strategies 21
3.2.5 Assessment of ICT internal governance 23
3.2.6 Assessment of ICT risk management framework 23
3.2.7 Assessment of ICT risk exposures and controls 24

Annex 1. Compliance table of the Guidelines 32

Annex 2. Country codes and acronyms of relevant competent authorities 38

Annex 3. Summary of CAs responses to benchmark questions 40

Annex 4. Self-Assessment Questionnaire for CAs 41

List of 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
EBA	European Banking Authority
ECB	European Central Bank
EEA	European Economic Area
ICAAP	Internal capital adequacy assessment process
ICT	Information and Communication Technology
LSI	Less Significant Institution
MS	Member State
N/A	Not Applicable
NCA	National Competent Authority
PRC	Ad hoc Peer Review Committee
PSD2	Payment Services Directive (Directive (EU) 2015/2366)
SAQ	Self-Assessment Questionnaire
SI	Significant Institution
SREP	Supervisory Review and Evaluation Process
SSM	Single Supervisory Mechanism
TIBER	Framework for Threat Intelligence-based Ethical Red Teaming

Executive Summary

The findings from the EBA peer review on the ICT risk assessment under the SREP suggest that competent authorities (CAs) across the EU have largely implemented the EBA Guidelines on ICT Risk Assessment under the SREP and applied the Guidelines in their supervisory practices. The CAs generally apply a risk-based approach to the supervision of ICT risk where the frequency and depth of the assessments correlate with the level of ICT risk of the institutions. The main challenges faced by CAs are building the necessary ICT supervisory capacity and expertise, applying proportionality in the assessment, and incorporating the ICT risk assessment into the overall SREP. No significant concerns regarding the ICT risk assessment under the SREP were identified in the course of the peer review, but the EBA makes a number of recommendations for further improvements of supervisory practices.

Information and communication technology (ICT) plays an important role in the functioning of credit institutions and ICT risk has become increasingly relevant and complex for individual institutions and for the banking industry as a whole. Against this background, the topic of ICT risk has been prominent in the EBA's regulatory and supervisory convergence work over the last years, and the EBA also developed guidelines to assist competent authorities in their assessment of ICT risk as part of the supervisory review and evaluation process (SREP).

The objective of the EBA Guidelines on ICT Risk Assessment under the SREP (EBA/GL/2017/05, 'the Guidelines') that apply since 1 January 2018 is to promote common procedures and methodologies for the assessment of ICT risk in the context of the SREP.

COVID-19 has raised further attention to ICT risks given that credit institutions had to rapidly adapt their technical infrastructures and way of working in response to the pandemic, and the crisis thus acted as a catalyst for digital transformation more generally. The reliance of the financial system on technology and the scope for cyber vulnerabilities have further increased. Against this background, at the end of 2021, the EBA launched a peer review of the assessment by competent authorities of ICT risk as part of the SREP. The peer review is focused on three key areas:

(1) The assessment of institutions' ICT internal governance (section 2.3 of the Guidelines);

(2) The assessment of institutions' ICT risk management framework (section 2.4 of the Guidelines); and

(3) The assessment of institutions' ICT security risk exposures and controls (section 3.3.4 (b) of the Guidelines).

The peer review was performed by the EBA's Ad hoc Peer Review Committee (PRC) following the process in Article 30 of the EBA Regulation and the EBA peer review methodology. This report summarises the conclusions of the peer review focusing on the general implementation of the

Guidelines and the supervisory practices in ICT risk assessment under the SREP, in particular with regards to the three above key areas.

In view of the EBA's statutory task of fostering convergence of supervisory practices across the EU, the report also identifies some good supervisory practices observed during the analysis that are recommended for consideration by CAs (e.g. building up and further development of knowledge and dedicated ICT skills, use of horizontal analyses). The report also indicates areas where relevant authorities should consider improving their practices (e.g. use of self-assessment questionnaires, IT landscape analyses, supplementing supervisory work with automated tools where available).

Based on the outcomes of the peer review, the PRC concludes that despite some exceptions and some delays in the implementation of the Guidelines by a small number of CAs, the Guidelines have been largely implemented by the CAs and applied in their supervisory practices. Nevertheless, this implementation is hindered by significant challenges. The main challenges faced by CAs are building the necessary ICT supervisory capacity and expertise, applying proportionality in the assessment, and incorporating the ICT risk assessment into the overall SREP.

The CAs have applied a risk-based approach to the supervision of ICT risk where the frequency and depth of the assessments correlate with the level of ICT risk in the institutions. The COVID-19 pandemic impacted the supervisory work and led some of the CAs to make use of the pragmatic SREP approach in 2020.[1] Over the course of the pandemic additional ad hoc work was also conducted by CAs, for example on cyber security and business continuity risks.

The PRC also recommends that the EBA, as part of its future review of the Guidelines and of the SREP Guidelines (EBA/GL/2014/13), consider including in the review an enhanced guidance for the application of proportionality, and further elaborate some ICT risk sub-categories as well as the methodology on how to incorporate the ICT risk assessment and scores into the overall SREP.

[1] See EBA Guidelines on the pragmatic 2020 supervisory review and evaluation process in light of the COVID-19 crisis

1. Background and rationale

1.1 Introduction

1. As set out in Article 30 of the EBA Regulation, the EBA shall periodically conduct peer reviews of some or all of the activities of competent authorities (CAs) within its remit, to further strengthen consistency and effectiveness in supervisory outcomes. This peer review focuses on the assessment of CAs' supervisory approach regarding the EBA Guidelines on ICT Risk Assessment under the SREP.

1.2 EBA Guidelines on ICT Risk Assessment under the SREP

2. The growing importance and rising complexity of ICT risk within the banking industry and in individual institutions, as well as the increasing potential adverse prudential impact from this risk on an institution and on the sector as a whole, prompted the EBA to develop guidelines on the common assessment of ICT risk in the context of the supervisory review and evaluation process (SREP).

3. The EBA published its ICT Risk Assessment Guidelines under the SREP[2] (EBA/GL/2017/05, 'the Guidelines') in 2017 for application as of 1 January 2018. The guidelines provide common procedures and methodologies to assist competent authorities in their assessment of the ICT risk under the SREP.

4. The guidelines are structured around three main parts: (i) the general provisions for applying the guidelines; (ii) the assessment of the institution's ICT governance and strategy; and (iii) the assessment of ICT risk and the controls in place at the institution. The guidelines are complemented by an ICT risk taxonomy, which includes a list of five ICT risk categories and a non-exhaustive list of examples of material ICT risks.

5. The guidelines form an integral part of the EBA Guidelines on common procedures and methodologies for the SREP[3] (EBA/GL/2014/13, 'the SREP Guidelines') and explain how the assessment of ICT risk contributes to the overall SREP assessment of an institution. In particular, (1) the assessment of ICT risk contributes to the assessment of operational risk, which is assessed as part of the assessment of risks to capital, (2) the assessment of the institution's governance and strategy on ICT feeds into the overall assessment of internal governance and institution-wide controls, and (3) the assessment of an institution's ICT strategy and its

[2] EBA Guidelines on ICT Risk Assessment under the SREP (EBA/GL/2017/05): https://www.eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-on-ict-risk-assessment-under-the-srep

[3] EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing (EBA/GL/2014/13): https://www.eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-for-common-procedures-and-methodologies-for-the-supervisory-review-and-evaluation-process-srep-and-supervisory-stress-testing

alignment with the institution's business strategy feeds into the business model analysis under the SREP.

1.3 Competent Authorities notification of Comply or explain

6. Regulation (EU) No 1093/2010 establishing the EBA requires that competent authorities and financial institutions make every effort to comply with the EBA guidelines and recommendations (Article 16).

7. EBA Guidelines and recommendations are formally issued only once they are published in all relevant EU official languages on the EBA website. Within 2 months after this publication, competent authorities across the EU must inform the EBA whether they comply or intend to comply with the guidelines or recommendations. If a competent authority does not comply or does not intend to comply, it must inform the EBA of this and state reasons for non-compliance, as prescribed by the 'comply or explain' principle. If specified in the guidelines or recommendations, financial institutions might also have to report whether or not they comply.

8. The EBA publishes for each guideline a table that summarises the compliance status and lists the feedback received from each competent authority across the EU. This information is also published in the EBA Annual Report so that the European Parliament, Council and Commission can be informed of what guidelines and recommendations were published over the course of the year, as well as which EU competent authorities are complying or intend to comply.

9. The EBA published the compliance table of the Guidelines, based on feedback received from CAs – see Annex 1.

1.4 Scope and methodology

10. In terms of scope, the peer review focuses on the assessment of the CAs' supervisory approach regarding the Guidelines, taking into account the outcomes of the EBA supervisory convergence report 2020 and the 2022 European Supervisory Examination Programme for prudential supervisors.

11. In addition to the above, the peer review assesses competent authorities' approaches to the supervision of credit institutions by focusing on three key areas. These were chosen based on (a) the outcomes of the EBA supervisory convergence report 2020 and the 2022 European Supervisory Examination Programme for prudential supervisors, (b) the ongoing discussions across the relevant EBA sub-structures, and (c) the upcoming areas of focus of DORA[4].

12. The three key areas of the Guidelines (and their respective aspects) covered during this peer review are the following: assessment of institutions' ICT internal governance (section 2.3 of the

[4] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014

Guidelines), assessment of institutions' ICT risk management framework (section 2.4 of the Guidelines), assessment of institutions' ICT security risk exposures and controls (section 3.3.4 (b) of the Guidelines).

13. The peer review is based on a one-year period from 1 January 2021 to 31 December 2021[5].

14. This peer review was performed by the Ad hoc Peer Review Committee (PRC), comprising four representatives from CAs and three EBA staff members. The PRC followed the process outlined in Article 30 of the EBA Regulation and in the EBA peer review methodology.

15. The PRC developed a self-assessment questionnaire (SAQ) (as included in Annex 4), to be completed by the CAs, which are competent for supervising credit institutions authorised in accordance with the Capital Requirements Directive (Directive 2013/36/EU (CRD)).

16. Responses to the questions in the self-assessment questionnaire (SAQ) were assessed against the cited benchmarks devised to assess the supervisory practice followed by each competent authority, in accordance with Article 19 of the EBA Peer Review Methodology Decision (EBA DC 2020 327).

17. For benchmarking purposes, the following grade-scales were used:

- **Fully Applied**: A provision is considered to be 'fully applied' when all assessment criteria as specified in the benchmarks are met without any significant deficiencies.
- **Largely Applied**: A provision is considered to be 'largely applied' when some of the assessment criteria are met with some deficiencies, which do not raise any concerns about the overall effectiveness of the competent authority, and no material risks are left unaddressed.
- **Partially Applied**: A provision is considered to be 'partially applied' when some of the assessment criteria are met with deficiencies affecting the overall effectiveness of the competent authority, resulting in a situation where some material risks are left unaddressed.
- **Not Applied**: A provision is considered to be 'not applied' when the assessment criteria are not met at all or to an important degree, resulting in a significant deficiency in the application of the provision.
- **Non-contributing:** A competent authority shall be classified by the PRC as 'non-contributing' if it has not provided its contribution within the prescribed deadline**.**

The relevant findings are presented in Chapter 3 of this report and summarised in Chapter 2.

[5] It is acknowledged that due to the COVID-19 pandemic CAs might have experienced potential differences in ICT supervision for example due to the cancellation of on-site inspections or on-site work being conducted remotely (impacting for example the assessment of physical security measures), hence a two-year period was used where deemed relevant (as indicated accordingly in the relevant sections of the report).

2. Peer review outcomes and recommendations

18. All EEA CAs responsible for the prudential supervision of credit institutions and the ECB-SSM as the addressees of the Guidelines have provided responses to the benchmark questions in the SAQ. The responses as provided by the CAs are summarised in Annex 3 and suggest that the Guidelines with some exceptions have been either fully or partially applied by the CAs in their jurisdictions.

19. The responses to the SAQ reflect the situation at the cut-off date for the peer review (December 2021) and cover the period of 1 January 2021 to 31 December 2021 (or for some questions, as indicated, the period of 1 January 2020 to 31 December 2021). Therefore, the analysis does not include any more recent developments or changes in the CAs' methodologies or supervisory practices since end December 2021. Whereas for benchmarking questions the response options included the possibility for competent authorities to reflect partial compliance, for some other questions the response option of 'not yet, but planning to' can reflect different stages of implementation.

20. The PRC reviewed the self-assessments provided by the CAs with a view to ensuring consistency of the responses and benchmarks and reflected on the additional details provided by the CAs in response to follow-up questions. The result of the final assessment is summarised in section 2.1. The review of the self-assessment suggests that despite the Guidelines being largely implemented, CAs face significant challenges that hinder effective compliance.

2.1 Summary of findings

2.1.1 General implementation of the Guidelines

21. Based on the outcomes of the assessment of the CAs' responses to the SAQ and additional information provided in response to follow-up questions, the PRC concludes that despite some exceptions and some delays in the implementation of the Guidelines by a small number of CAs, the Guidelines have been largely implemented by the CAs and applied in their supervisory practices. Nevertheless, this implementation is hindered by significant challenges as explained below.

22. The majority of CAs have fully applied the Guidelines in their jurisdictions, with the requirements provided in the Guidelines being also incorporated in both SREP methodologies and manuals. Except one CA, almost all the authorities use a dedicated methodology for ICT risk assessment.

2.1.2 Challenges faced in the assessment of ICT risks

23. The lack of sufficient skilled resources is identified as the main challenge by most of the CAs. ICT risk assessment requires specific skills such as knowledge and expertise on ICT systems and environments, as well as the ability to analyse technical information to identify unmitigated risks and ineffective controls. And due to the rapidly evolving landscape, there is the need for a continuous update and learning process. The building up of knowledge and dedicated skills also remains challenging and hiring adequate resources on the market is difficult as they are scarce and in high demand, including by the private sector.

24. The incorporation of ICT risk in the overall SREP in an objective and consistent way is also perceived as a challenge. As there is no detailed guidance on the incorporation of the scores, the approaches may vary. CAs underline the need to improve the effectiveness and consistency in the assessment and scoring, and to avoid underweight of ICT risk in overall scores.

25. The application of proportionality in the assessment of ICT risk under the SREP is deemed challenging by many CAs, both in view of the amount of institutions under their remit, and/or the heterogeneity of those institutions. In particular, applying proportionality in assessing in depth all relevant ICT risk subcategories is deemed difficult by some CAs. Including more guidance to apply the proportionality principle in the Guidelines has been suggested.

2.1.3 Supervisory practices in ICT risk assessment under the SREP

26. Under the Guidelines, the ICT risk assessment feeds into the assessment of operational risk and the assessment of the business model, internal governance and risk management. Most of the authorities (23 CAs) have developed a methodology to assign ICT risk scores based on the Guidelines. However, the incorporation of ICT risk scores into the overall SREP is perceived as a challenge due to lack of detailed guidance.

27. The majority of CAs reported assessing ICT Risk under the SREP in compliance with the Guidelines for more than 75% of the institutions under their supervision in the last two years (covering the period of January 2020 to December 2021). The COVID-19 pandemic impacted the supervisory work and led some of the CAs to make use of the pragmatic SREP approach in 2020. Over the course of the pandemic also additional ad hoc work was conducted by CAs for example on cyber security and continuity risks.

28. Several CAs consider ICT risk as material for all institutions by default. Where ICT risk is assessed as material, it is assessed as a subcategory of operational risk and often scored on an individual basis (based on Table 1 of the Guidelines and considering the level of risk and the level of control), though not in all cases. In most of the cases, the ICT risk score is incorporated in the overall operational risk score based on expert judgement.

29. Most CAs perform a regular oversight of the implementation of ICT strategies by credit institutions. CAs highlighted a number of challenges faced by institutions in the implementation

of ICT strategies, mostly related to legacy systems, lack of expertise and dependencies on third parties.

30. In terms of enforcement, CAs generally issue findings and/or recommendations to institutions when deficiencies are identified in the ICT strategy framework and implementation, the ICT risk management framework, ICT internal governance and ICT risk exposures and controls.

31. In general, CAs use the guidance included in the Guidelines for their assessment of ICT risk management under the SREP. If additional criteria are used, they are mostly set out in the national regulatory frameworks, and often referencing other EBA Guidelines or international standards (COBIT, ISO) or guidance (FSB, BCBS).

32. With regards to the methodologies to rate, measure, and benchmark risks and controls for the sub-category of ICT security risk, practices are still evolving with just over half of CAs having in place a dedicated methodology, and a third of CAs planning to develop one.

33. Overall, as regards to the ICT risk assessment under the SREP a relatively high compliance with the Guidelines is reported by CAs, both for their application and in terms of coverage of the five ICT risk sub-categories outlined in the Guidelines. Also, a relatively high number of institutions has been assessed under the Guidelines over the last two years, although with application of proportionality as regards to the frequency and depth of the assessment. This is considered a high score, taking into account the challenges reported by CAs of a lack of supervisors with specialized ICT skills, as regards to reviewing ICT risks for a high number of banks with limitations in the information provided by institutions, and other inherent challenges on incorporating the ICT risk assessment into the SREP.

2.2 Good practices developed by competent authorities

34. The lack of skilled resources is identified as the main challenge by most of the CAs. All CAs have in place forms of activity to improve the levels of expertise and skills in general supervisory staff overall. On top of training, some CAs include general staff in ICT risk supervisory work and/or on-site inspections (20 CAs) and in external training (19 CAs). Other ways of increasing expertise are participation of general staff in working groups with mixed expertise (also at international level, e.g. ESAs working groups), general workshops, and forms of mentoring. Other initiatives are the set-up of internal networks between supervisors and policy experts, and thematic reviews on ICT risk.

35. To support the incorporation of the ICT risk assessment in the SREP, which is identified as the second main challenge they faced, some CAs use a dedicated methodology to facilitate the assessment process (20 CAs) or make use of the monitoring of ICT risk related metrics or key indicators (18 CAs). Some CAs (9) indicate the use of IT solutions to facilitate the assessment process.

36. Some CAs make use of ICT self-assessment questionnaires to be completed by the institutions on a regular (often annual) basis. The self-assessment questionnaires are assessed by CAs and

used for horizontal analysis and benchmarking purposes, and as input into the SREP. The self-assessment questionnaire can be adapted to different types of institutions, for example by using more extensive versions for large and complex institutions, and simplified questionnaires for smaller and less complex institutions. The use of self-assessment questionnaires can facilitate the assessment of ICT risks and the level of controls for a large number of smaller and less complex institutions in view of supervisory resource constraints, enhance convergence in the assessment across institutions, and help to gather more granular information from institutions in a uniform way. As CAs challenge the self-assessments (based on on-site or off-site supervisory work at institution-specific and/or horizontal level) they will become more realistic over time.

37. One CA reported performing an IT landscape analysis for all credit institutions within its jurisdiction. The analysis forms part of the review of the critical ICT systems and services of institutions and is aimed at identifying ICT risks with a potential significant prudential impact on the institutions. For the exercise, a granular, structured and fact-based questionnaire is used to collect comparable data related to critical ICT systems. The data are consolidated, visualized and analysed on a bank-specific, horizontal (cross-institutional) and vertical level (by business processes/services or risk aspect). The results provide insights into the criticality and interdependencies between business processes, the related critical IT systems and key IT providers. The outcomes are used in the assessment and scoring of ICT sub-categories in the SREP. The IT landscape analysis can be a good tool for CAs for the assessment of smaller institutions with comparable business models and a simple IT architecture. The analysis allows to have a better understanding of inherent ICT risk (criticality, complexity, interdependencies) and ICT outsourcing concentration risk. It can support other supervisory tasks (on-site preparation, monitoring of ICT change projects, business continuity, recovery and resolution planning), and to be in a better position to challenge institutions' ICT risk and ICT control self-assessments. It can also assist CAs to be more proactive when cyber threats/attacks occur.

38. One CA reported performing peer reviews and mutual comparisons of the maturity of ICT related processes and security technologies. The reviews are conducted in the context of on-site inspections at the largest banks. The differences are evaluated and supervisory tools used for low performance entities. The supervisory expectations with regards to ICT security controls are strengthened according to the evolution of the cyber threat landscape. Developments at institutions are monitored on a regular basis accordingly to ensure ICT security controls and mitigations are still effective in view of the evolution of the cyber threat landscape.

39. For the purpose of assessing the ICT strategies of institutions in terms of development, adequacy and implementation, several CAs assess whether the monitoring of the implementation of the ICT strategy is based on quantitatively measurable indicators which allow for a meaningful review of the achievement of the goals in the sense of a target-actual comparison. This is deemed particularly relevant in view of the challenge identified by several CAs that the lack of a concrete implementation plan and timeline for the ICT strategy causes difficulties for the institution and the CA to monitor its implementation.

2.3 PRC recommendations

2.3.1 Recommendations to CAs

40. Considering that ICT risk assessment requires specific skills and expertise, the building up of the necessary capacity and expertise is key to effective supervision in this area. It is also important to keep the required skillset up to date in view of the changing ICT and regulatory landscape, for example in light of the upcoming DORA. Training curriculums on ICT risk should be developed where not yet available. These can be supplemented with other initiatives to enhance the expertise of ICT experts and build up the knowledge of general supervisors in the area of 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.

41. The PRC recommends CAs which do not perform horizontal analysis as part of their supervision of ICT risk, to set up this comparison, in particular for detecting outliers, and assuring a level playing field in their jurisdiction. In addition, thematic horizontal analyses can be performed in specific ICT risk areas based on a risk-based approach and according to supervisory priorities. The use of horizontal analyses is 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.

42. In order to allow for a proportionate approach to the ICT risk assessment under the SREP, in particular to facilitate and enhance the effectiveness and efficiency of their work, the PRC recommends CAs to make use of available tools such as self-assessment questionnaires, IT landscape analyses and to support the supervisory work with automated tools where available.

2.3.2 Recommendations to the EBA

43. The PRC recommends to the EBA, as part of its future review of the Guidelines, which can take place after the finalisation of DORA Level 1 and Level 2 legal texts, to consider the following:

    a. Incorporating the Guidelines into the general SREP guidelines to make general supervisors more aware of and engaged with the need to apply the guidelines.

    b. Developing the application of proportionality for all institutions, including smaller and less complex institutions, for which the methodology is less developed. It is not always feasible to assess in depth all relevant ICT risk subcategories for all institutions. This could be aligned with the proportionality approach envisaged in the upcoming Digital Operational Resilience Act (DORA).

    c. Elaborating the methodology on how to incorporate the ICT risk score into the SREP, considering the relatively low impact on the overall operational risk score.

d. Enhancing the guidance in section 3.2.2 of the Guidelines for competent authorities to form an opinion on which ICT systems and services are critical for the adequate functioning, availability, continuity and security of the institution's essential services including considering to define more concrete thresholds for the assessment of the criticality.

e. Further elaborating on some risk categories that are less developed than others, namely:

- ICT data integrity risk level and risk controls – in view of consistency with BCBS 239[6] and expectations, and provision of additional guidance and assessment criteria for the data integrity sub-category in Annex to the Guidelines. It should be emphasized however that BCBS 239 and the ICT data quality subcategory do not cover the same scope and the same objective.

- ICT change risk level - how to identify and measure this risk in practice.

f. For the ICT risk sub-categories ensuring a better harmonization (i) between risk-level and risk-control sub-categories; (ii) with CRR Article 324; (iii) with the EBA/GL/2019/04[7]; (iv) with the EBA/GL/2019/02[8]; and (iv) with PSD2 Article 95; and updating the guidance in view of DORA.[9]

g. Adding to the assessment of ICT strategies whether the goals of the ICT strategy of the institution contain quantitatively measurable criteria and a process to monitor and measure the effectiveness of the implementation of the ICT strategy.[10]

[6] Basel Committee on Banking Supervision, Principles for effective risk data aggregation and risk reporting, January 2013.

[7] EBA Guidelines on ICT and security risk management (EBA/GL/2019/04): https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management

[8] EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02): https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

[9] It was suggested to maintain the overall ICT risk taxonomy unchanged in view of the substantial impact of changes on the existing methodologies and tools.

[10] In line with the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04) paragraph 6.

3. Assessment of practices of competent authorities

44. This section provides a detailed overview and a PRC analysis of the CAs' responses to the SAQ. The analysis follows the structure of the SAQ, which is organised into the following main blocks: 1) Implementation of the EBA Guidelines on ICT risk assessment under the SREP; and 2) Supervisory practices in ICT risk assessment under the SREP.

3.1 Implementation of the EBA Guidelines on ICT Risk assessment under the SREP

3.1.1 General implementation

45. All CAs have incorporated the Guidelines into their SREP methodology (at least partially for 9 CAs among 31).

46. Except one CA, all the authorities have set up a dedicated methodology for ICT risk assessment (at least partially for 8 among 31 authorities).

3.1.2 Proportionality

47. Most of the CAs indicate incorporating proportionality for ICT risk in their methodology. The ICT risk profile triggers the frequency, scope and depth of the ICT risk assessment (number of questions/indicators, areas/scope to be covered). The ICT risk profile takes into account the business model/activities, the size and ICT complexity of the institution and the number of on-line channels. At the same time, applying proportionality in assessing in depth all relevant ICT risk subcategories is perceived as a challenge by some CAs.

48. For all the SSM SIs, all ICT risk sub-categories are assessed at least at a high level on an annual basis. Considering the scope of the sub-categories, the in-depth assessment of the sub-categories is distributed across several cycles. The choice of which sub-category to assess depends on the SSM Priorities, the ICT risk profile, business model, type of activities of the bank as well as any other relevant information.

49. For the LSIs, the SSM CAs mainly apply the SSM SREP methodology for LSIs. This methodology incorporates proportionality by distinguishing High Priority LSIs (HP-LSIs) and non-High Priority LSIs (non-HP-LSIs) which triggers the number of indicators to analyse for each IT risk sub-category, as well as affecting the recurrence of the SREP assessment itself (annually, every two years or every three years).

50. Two CAs indicate incorporating proportionality differently, one by using the ratio of ICT related losses in total losses, the other when calculating the final score for ICT risk.

3.1.3 Incorporating the assessment of ICT risks in the SREP

51. Most of the authorities consider ICT risk as a sub-category of operational risk within the SREP framework. However, the horizontal topics (ICT governance, ICT risk management and ICT strategy) are taken into account for the assessment of business model, internal governance, and risk management.

52. One CA applies a different methodology to assess the impact of ICT risks on business model and profitability, based on an assessment of digitalization strategies, although it is connected to the assessment under operational risk under the Guidelines in what concerns the ICT strategy.

53. One CA performs the ICT risk assessment for the SREP as a separate task, but the findings and elements of the ICT risk assessment are inserted into the general SREP assessment table as one element.

3.1.4 Assessing ICT risks in the SREP as a sub-category of operational risk

54. Whilst generally CAs should assess sub-categories of ICT risks as part of the main categories (i.e. ICT risk will be assessed as part of operational risk), where CAs deem some sub-categories material, they may assess such sub-categories on an individual basis. To this end, should ICT risk be identified as a material risk by the CA, the Guidelines also provide a scoring table (Table 1) that should be used to provide a stand-alone sub-category score for ICT risk following the overall approach to scoring the risks to capital in the SREP Guidelines.

55. 14 CAs indicate having set up a methodology to assign an ICT risk score based on Table 1 of the Guidelines, 10 CAs at least partially, 2 CAs plan to set up such methodology, and 4 CAs do not.

56. The authorities which set up a methodology to assign an ICT risk score make use of Table 1 of the Guidelines. The SSM SREP methodology (for SIs) defines an ICT risk level and an ICT risk control score. The ICT risk level score is determined for each sub-category based on the inherent risk level based on several quantitative indicators aimed at measuring that risk. The risk control scores are based on the maturity of several specific controls to be implemented by the supervised entities. The list of these controls is not considered as exhaustive, so other mitigating controls/methods are also considered for the scoring. The SSM SREP methodology for LSI does not set up a methodology to assign an ICT risk score, but the operational risk scores (for risk level and risk control) take into account ICT risks. One authority assigns a dedicated/stand-alone score for ICT risks, and another one is planning to do so.

3.1.5 ICT risks in the score for operational risk

57. The operational risk score itself is derived from a risk level and a risk control score. Most of the authorities indicate incorporating the ICT risk score in the overall operational risk score based on expert judgement (in some cases considering the significance of ICT risks). Some authorities define rules for weighting the ICT risk score within the overall operational risk score (24% for one CA, average of all operational risk category scores, the operational risk score cannot be

better than the ICT risk score). One CA uses a weighted operational risk score taking into account ICT risks.

3.1.6 Inputs used in the assessment of ICT risks

58. In the assessment of the ICT risk under the SREP, inputs from third parties, such as auditors, can be used for certain provisions of the Guidelines. Except 3 CAs, all the authorities indicate using (or planning to use) inputs from third parties.

59. Where CAs use third-party inputs, most of them consider external audit reports (22 CAs) as well as internal audit reports in some cases (9 CAs). Some additional third-party reports (penetration tests exercises, certification reports, SWIFT Customer Security program (CSP) compliance reports) are also mentioned by some authorities.

60. Inputs from other supervisory processes/tools are also used. Most of the CAs use input from on-site inspections; off-site work; outcomes of self-assessment questionnaires; and cyber incident reporting. 3 CAs do not use the outcomes of self-assessments. One CA relies only on cyber incident reporting. 11 CAs use the outcomes of threat-led penetration tests (e.g. TIBER) for the assessment of ICT risks.

61. Other inputs used in the assessment of the ICT risk under the SREP are regular meetings with the institutions, regulatory reporting (including reporting on losses), (PSD2) incident reporting and outsourcing contracts' review.

62. Most of the authorities consider the inputs from all supervisory processes/tools in the actual SREP assessment based on expert judgement.

3.1.7 Challenges faced in the assessment of ICT risks

63. CAs were asked to list, in terms of importance, the challenges they face in the assessment of the ICT risk under the SREP under the Guidelines (practical, organizational, or other) and to explain how they address these challenges.

64. The lack of skilled resources is identified as the main challenge by most of the CAS, followed by the incorporation of ICT risk in the overall SREP (with the need to improve the effectiveness and consistency in its assessment and no underweight of ICT risk in overall scores) and adapting to rapidly changing new technologies.

65. Top level challenges:

- Resources: the ICT risk assessment requires specific knowledge and expertise on ICT systems, environments and controls that banking supervisors' profiles do not always have to the same extent. The building up of knowledge and dedicated skills remains challenging also in view of the rapidly evolving landscape. ICT risk assessment also requires the ability to analyse technical information to identify unmitigated risks and ineffective controls.

- Some aspects of the ICT SREP: incorporation of the ICT SREP into the overall SREP in an objective and consistent way and with no underweights of ICT risk in the overall SREP scores, the need for rapid adaptations to the fast-changing context (frameworks, regulation, etc.).

- The quality of the information available about ICT risk, in terms of qualitative nature, completeness, uniformity, meaningfulness.

66. Medium-level challenges:

- Some aspects of the external context that increase the ICT risk of the banks: the increasing adoption of new technologies and the constant evolution of the threats landscape.

67. Low-level challenges:

- Some aspects of ICT risk supervision: risk assessment of LSIs, of some ICT risk profiles, application of proportionality, activities planning, numerous follow-ups, the need to deal with many regulations by different authorities (overlapping requirements), broad definitions.

3.1.8 Horizontal analysis in the assessment of ICT risks

68. Most of the CAs (25) indicate performing horizontal analysis: for 23 CAs the analysis is effective, whereas for 2 CAs it is planned or in progress. 6 CAs do not perform horizontal analysis.

69. The main tools used for the analysis are self-assessment questionnaires and risk assessment, but there are other input tools used by fewer CAs (incident reporting, ICT strategy documents and the SSM IT Risk Analysis (SITRA) Tool), whereas the most applied type of horizontal analysis is the peer comparison.

70. Overall, with horizontal analysis CAs pursue a wide range of main purposes: sectorial overview, benchmarking, detecting capabilities/deficiencies/preparedness, outliers' detection and risk concentration; in some cases, horizontal analysis is reported as being used to inform supervisory activities.

3.2 Supervisory practices in the ICT risk assessment under the SREP

3.2.1 General supervision, prioritization and resources

71. The vast majority of CAs (30 out of 31) perceive the supervision of ICT risk as important or very important.

72. According to the supervisory priorities defined, two thirds of CAs consider their resources (horizontal and off/on-site) adequate or mostly adequate, whereas one third (11 CAs) consider their resources not adequate with improvements needed.

73. All the CAs that seek more resources need ICT risk specialists. Expertise is often needed in some specific ICT risk subcategories (namely ICT security, ICT availability and continuity, ICT outsourcing as well as emerging ICT risks).

74. The main difficulties perceived in hiring staff with adequate expertise are limited availability in the labour market (absolute resource scarcity and/or high demand of the market) (9 CAs out of 10), competitive terms of employment (e.g. salaries) (4 CAs out of 10) and insufficient interest for the sector (3 CAs out of 10).

75. All CAs have in place forms of activity to improve the levels of expertise and skills of the general supervisory staff. The most relevant activities are training (23 CAs), inclusion of general staff in the ICT risk supervisory work/on-site inspections (20 CAs) and external training (19 CAs).

76. Other forms of activity to improve the levels of expertise are participation of general staff in working groups with mixed expertise (also at international level, e.g. ESAs working groups), general workshops, and forms of mentoring.

77. If ICT training is provided to general supervisory staff, CAs were asked to indicate if they have a training curriculum, the total number of training sessions provided in 2021, and the number of trained supervisors in 2021.

- 10 CAs out of 23 have a training curriculum.
- In 2021, the average number of training sessions provided was 7 and the average number of trained supervisors was 92.

78. CAs were asked how they see the importance of the supervision of ICT risk in their jurisdiction in terms of supervisory priorities (based on their CA's work programme and identified priorities) for the last two years.

- 22 CAs out of 31 assigned high importance
- 9 CAs assigned medium importance
- No CAs assigned low importance

79. CAs were asked if they take any specific initiatives to support the incorporation of the ICT risk assessment in the SREP.

- The vast majority of CAs (30 CAs) take specific initiatives.

- The most frequent initiatives are ICT related training provided to supervisory staff (20 CAs), use of a dedicated methodology to facilitate the assessment process (20 CAs), monitoring of ICT risk related metrics or key indicators (18 CAs).

- 9 CAs indicate the use of IT solutions to facilitate the assessment process.

3.2.2 Assessment of ICT risk

80. CAs were asked for how many institutions under their supervision they assessed ICT risk in compliance with the Guidelines in the last two years (covering the period of January 2020 to December 2021).

- 19 CAs assessed ICT risk for more than 75% of the institutions

- 6 CAs assessed ICT risk for 50% to 75% of the institutions

- 6 CAs assessed ICT risk for less than 50% of the institutions

81. As explained in section 3.1.2, CAs generally follow a risk-based approach using the ICT risk profile and SREP categorization to trigger the frequency, the scope and the depth of the ICT risk assessment. Four CAs explicitly made reference to the pragmatic SREP approach used in 2020 in view of the COVID-19 pandemic.

82. Several CAs request institutions to complete IT risk self-assessment questionnaires on an annual basis. The self-assessment questionnaires are assessed by CAs and used for benchmarking purposes and as input into the SREP.

3.2.3 Assessment of materiality of ICT risk and ICT risk taxonomy

83. CAs were asked for how many of the institutions under their supervision they consider ICT risk as material (applying the criteria set out in paragraph 17 of the GLs and/or additional criteria).

- 22 CAs assessed ICT risk as material for more than 66% of the institutions

- 4 CAs assessed ICT risk as material for 33% to 66% of the institutions

- 4 CAs assessed ICT risk as material for less than 33% of the institutions

84. Several CAs confirmed they consider ICT risk as material for all institutions by default. This implies that ICT risk is assessed as a subcategory of operational risk for all institutions though the assessment will be adapted according to the risk profile and business model of the institution and the materiality of the subcategories of ICT risk. For determining the frequency of the assessment, one CA applied additional criteria with regards to the significant operational or security incidents, and important changes in the ICT systems of the institution.

85. In terms of additional criteria used by CAs for assessing the materiality of ICT risk of institutions (besides those set out in paragraph 17 of the Guidelines), reference was made to the ICT risk

profile, complexity of business processes and IT systems. Also the use of forward-looking (which inherent risks are likely to materialize in the future) and backward looking (which risks have materialized in the past) perspectives in order to assess ICT risk levels were mentioned, as well as the use of other sources of information such as PSD2 reporting containing information on operational incidents.

86. When CAs assess ICT risk as material, they can provide a standalone score for ICT risk as an individual sub-category of operational risk. From the responses it appears that for institutions for which ICT risk is assessed as material, CAs provide a standalone score for ICT risk, though not in all cases.

- 17 CAs scored ICT risk as an individual sub-category of operational risk for more than 66% of the institutions for which IT risk is considered as material
- 4 CAs scored ICT risk as an individual sub-category of operational risk for more than 33% and less than 66% of the institutions for which IT risk is considered as material
- 9 CAs scored ICT risk as an individual sub-category of operational risk for less than 33% of the institutions for which IT risk is considered as material

87. Many CAs (27) use the list of ICT risk sub-categories and risk scenarios set out in the Annex of the Guidelines either fully (15 CAs) or partially (12 CAs). A few CAs (4) have set out additional ICT risk sub-categories, including ICT strategy and governance, internal ICT audit and ICT risk management.

88. CAs were asked if any of the ICT risk sub-categories and risk scenarios set out in the Annex of the Guidelines should be considered for deletion or improvement. 3 CAs suggested improvements. Suggestions include to provide additional guidance and assessment criteria for the data integrity sub-category. It was also pointed out that data integrity as part of data quality is only partly related to ICT risk. Another proposal was to ensure a better harmonization (i) between risk-level and risk-control sub-categories; (ii) with CRR Article 324; (iii) with the EBA/GL/2019/04; and (iv) with PSD2 Article 95. It was also referred to the possible future evolution of the risk scenarios stemming from the implementation of FinTech technologies. Finally, it was pointed out that whereas the risk sub-categories are not mutually exclusive, it would be prudent to leave the ICT risk taxonomy unchanged as changing this would have substantial repercussions for the existing methodologies and tools.

3.2.4 Assessment of ICT strategies

89. CAs were asked for how many of the institutions under their supervision they assessed (in compliance with the Guidelines) the development, adequacy and implementation of ICT strategies defined by credit institutions in the last two years.

- 16 CAs assessed ICT strategies for more than 75% of the institutions

- 6 CAs assessed ICT strategies for 50% to 75% of the institutions
- 9 CAs assessed ICT strategies for less than 50% of the institutions

90. Most CAs (25) identified shortcomings or deficiencies with regards to the ICT strategies of credit institutions. Almost all the CAs that identified relevant deficiencies in the ICT strategy framework and implementation submitted findings and/or recommendations to the credit institutions. Two CAs did not yet submit such findings and/or recommendations but are planning to do so.

91. Most CAs (26) apply the guidance referred to in section 2.2 of the Guidelines in their assessment of the development, adequacy and the implementation of ICT strategies defined by credit institutions, and four CAs are planning to do so.

92. If CAs use additional criteria for the assessment of ICT strategies, those are mostly set out in the national regulatory frameworks. Reference is also made to other EBA Guidelines (Guidelines on outsourcing arrangements, Guidelines on ICT and Security Risk management) and to international standards (COBIT, ISO) and the G7 Fundamental Elements of Cybersecurity for the Financial Sector. Some CAs indicated to assess in addition whether the goals of the ICT strategy of the institution contain quantitatively measurable criteria and a process to monitor and measure the effectiveness of the implementation of their ICT strategy in the sense of a target-actual comparison.

93. Many CAs (22) perform regular oversight of the implementation of ICT strategies by the credit institutions under their supervision. 9 CAs are not yet performing such regular oversight, 6 of which plan to do so in future.

94. CAs were asked what challenges they see for institutions in the implementation of their ICT strategies. CAs highlighted a number of challenges both related to the ICT strategy itself, and other challenges including structural challenges for their implementation. The issues related to the adaptation of legacy systems are identified as the main challenge by most of the CAS, followed jointly by the lack of skills and expertise and the dependencies on third parties (outsourcing). Many CAs also referred to the integration issues arising from mergers and acquisitions.

    Top 4 challenges:

    - Legacy systems
    - Lack of skills and expertise
    - Dependencies on third parties (outsourcing)
    - Integration issues from mergers and acquisitions

95. Other challenges identified by CAs in the institutions' implementation of ICT strategies include the adequacy of the ICT strategy and its alignment with the business strategy, the integration of

the ICT strategy with the business model and the lack of a concrete implementation plan and timeline causing difficulties for the institution and the CAs to monitor its implementation. Cost reduction constraints or inadequate human resources, the need for rapid adaption of the strategies and conversion to cloud strategies were also mentioned as challenges identified.

3.2.5 Assessment of ICT internal governance

96. CAs were asked for how many of the institutions under their supervision they assessed (in compliance with the Guidelines) institutions' ICT internal governance in the last two years.

- 17 CAs assessed ICT internal governance for more than 75% of the institutions
- 8 CAs assessed ICT internal governance for 50% to 75% of the institutions
- 6 CAs assessed ICT internal governance for less than 50% of the institutions

97. Most CAs (26) that identified relevant deficiencies in the ICT internal governance did submit findings and/or recommendations to the credit institutions. 4 CAs did not yet submit such findings and/or recommendations but are planning to do so.

98. Most CAs (28) apply the guidance referred to in section 2.3 of the Guidelines in their assessment of the ICT internal governance, and two CAs are planning to do so. One CA does not apply the guidance.

99. If CAs use additional criteria for the assessment of ICT internal governance, those are mostly set out in the national regulatory frameworks. Reference is also made to other EBA Guidelines (Guidelines on internal governance[11], Guidelines on ICT and Security Risk management[12]) and to international standards (COBIT, ISO) and the BCBS guidance on internal governance.

3.2.6 Assessment of ICT risk management framework

100. CAs were asked for how many of the institutions under their supervision they assessed (in compliance with the Guidelines) the institutions' ICT risk management framework in the last two years.

- 18 CAs assessed the risk management framework for more than 75% of the institutions
- 7 CAs assessed the risk management framework for 50% to 75% of the institutions
- 6 CAs assessed the risk management framework for less than 50% of the institutions

101. Most CAs (26) that identified relevant deficiencies in the ICT risk management framework did submit findings and/or recommendations to the credit institutions. Three CAs did not yet

[11] EBA/GL/2021/05

[12] EBA/GL/2019/04

submit such findings and/or recommendations but are planning to do so. Two CAs did not submit such findings and/or recommendations.

102. Most CAs (28) apply the guidance referred to in section 2.4 of the Guidelines in their assessment of the ICT risk management framework, and two CAs are planning to do so. One CA does not apply the guidance.

103. If CAs use additional criteria for the assessment of the ICT risk management framework, those are mostly set out in the national regulatory frameworks. Reference is also made to the EBA Guidelines on ICT and Security Risk management[13] and to international standards (COBIT, ISO), the BCBS 239 principles for effective risk data aggregation and reporting, the NIST framework, and the FSB Guidance on Supervisory Interaction with Financial Institutions on Risk Culture.

104. CAs were asked if they take into account expected and adverse scenarios for the assessment of whether the risk appetite and the ICAAP cover the ICT risks for the definition of the overall risk strategy and for the determination of internal capital. The majority of CAs (20) does not take into account expected and adverse scenarios for this assessment.

105. The CAs (11) that use expected and adverse scenarios for the above assessment consider a range of scenarios including loss of staff, loss of buildings, loss of external service providers, loss of IT systems, cyber-attacks, and data breach scenarios.

106. For the above assessment some CAs explicitly mentioned using stress testing scenarios from institutions. These scenarios can be included in the ICAAP, recovery plans, IT Business Continuity or Disaster Recovery Plans, or in the incident management process. Institutions can develop stress test scenarios for ICT risk and sometimes also use combined scenarios covering several possible operational risk and ICT risk events happening at the same time. One CA asked for more details from a sample of institutions on a specific type of scenarios (data leakage scenario) and whether it was considered in the institutions' crisis management framework. No supervisory stress testing related to ICT risk was used in this context.

3.2.7 Assessment of ICT risk exposures and controls

107. CAs were asked for how many of the institutions under their supervision they assessed (in compliance with the Guidelines) the institutions' ICT risk exposures and controls in the last two years.

- 17 CAs assessed the risk exposures and controls for more than 75% of the institutions
- 8 CAs assessed the risk exposures and controls for 50% to 75% of the institutions
- 6 CAs assessed the risk exposures and controls for less than 50% of the institutions

[13] EBA/GL/2019/04

108. Most CAs (26) that identified relevant deficiencies in the ICT risk exposures and controls submitted findings and/or recommendations to the credit institutions. Two CAs did not yet submit such findings and/or recommendations but are planning to do so. Three CAs did not submit such findings and/or recommendations.

109. Most CAs (27) apply the guidance referred to in section 3 of the Guidelines in their assessment of the ICT risk exposures and controls, and three CAs are planning to do so. One CA does not apply the guidance.

a. Review of the critical ICT systems and services

110. Most CAs (25) assessed (in compliance with the Guidelines) the methodology and processes applied by the institutions to identify the ICT systems and services that are critical, and three CAs are planning to do so. Three CAs do not perform such assessment in compliance with the Guidelines.

111. Some CAs (8) apply guidance beyond the provisions of the Guidelines in their assessment of the methodology and processes applied by institutions to identify the ICT systems and services that are critical, and two CAs are planning to do so.

112. If CAs use additional criteria for the assessment of the methodology and processes applied by institutions to identify the ICT systems and services that are critical, those are mostly set out in the national regulatory frameworks. Reference is also made to the EBA Guidelines on ICT and Security Risk management[14], to the EBA Guidelines on outsourcing arrangements[15], to PSD2, and to international standards (COBIT, ISO), the FSB Guidance on Supervisory Interaction with Financial Institutions on risk culture, the BCBS principles and the NIST framework.

113. One CA performed an IT landscape analysis for all credit institutions within their jurisdiction. The analysis forms part of the review of the critical ICT systems and services of institutions and is aimed at identifying ICT risks with a potential significant prudential impact on the institutions. For this exercise a granular, structured and fact-based questionnaire is used to collect comparable data related to critical ICT systems (complementary to the IT risk self-assessment questionnaire). The data are consolidated, visualized and analysed on a bank-specific, horizontal (cross-institutional) and vertical level (by business processes/services or risk aspect). The results provide insights into the criticality and interdependencies between business processes, the related critical IT systems and key IT providers. The outcomes are used in the assessment and scoring of ICT sub-categories in SREP.

114. CAs were asked if they face challenges in assessing the criticality of the ICT systems and services. Several CAs (18 of 31) faced such challenges.

[14] EBA/GL/2019/04

[15] EBA/GL/2019/02

115. The challenges faced by CAs in assessing the criticality of the ICT systems and services include the following:

- Lack of data provided by institutions and data quality issues
- Lack of specialist resources at the CAs
- Complexity of the ICT landscape, particularly in case of outsourcing
- Lack of complete overview of institutions on their IT infrastructure and its criticality
- Lack of detailed mapping of ICT systems to critical business functions
- Lack of proper IT asset inventory as a starting point for identifying critical assets
- Difference in terminology used at institutions regarding criticality levels

b. Identification of material ICT risks

116. Most CAs (29) apply the criteria set out in section 3.2 of the Guidelines for identifying material ICT risks. One CA is planning to do so.

117. Some CAs (6) apply guidance beyond the provisions of the Guidelines for identifying material ICT risks, and two CAs are planning to do so.

118. If CAs use additional criteria for identifying material ICT risks, those are mostly set out in the national regulatory frameworks. Reference is also made to the EBA Guidelines on ICT and Security Risk management,[16] to the SSM SREP methodology for LSIs, to international standards (COBIT, ISO), and the BCBS principles. The additional criteria used include the number of times risks materialized within the last year, and the number of times breaches of confidentiality took place. One CA considers all ICT risks as material.

119. CAs were asked if they face challenges in assessing the materiality of ICT risks. Several CAs (15 of 31) faced such challenges.

120. The challenges faced by CAs in assessing the materiality of ICT risks include the following:

- Lack of data and IT documentation from institutions
- Lack of specialist resources
- Tendency for the importance of ICT risk to be underestimated by institutions
- Quantification of ICT risks, their impact and materiality

[16] EBA/GL/2019/04

- Lack of quantitative indicators and thresholds for materiality
- Application of expert judgment
- Application of proportionality when assessing materiality of ICT risks

c. Assessment of the controls to mitigate material ICT risks

121. Most CAs (30) apply the criteria set out in paragraph 46 of the Guidelines for assessing the controls to mitigate material ICT risks. One CA is planning to do so.

122. Some CAs (9) apply guidance beyond the provisions of the Guidelines in their assessment of the controls to mitigate material ICT risks, and one CA is planning to do so.

123. If CAs use additional criteria for the assessment of the controls to mitigate material ICT risks, those are mostly set out in the national regulatory frameworks. Reference is also made to the EBA Guidelines on ICT and Security Risk management,[17] to the SSM SREP methodology for LSIs, to the EBA Guidelines on outsourcing arrangements,[18] to international standards (COBIT, ISO), and the BCBS 239 principles for effective risk data aggregation and risk reporting.

124. One CA reported performing peer reviews and mutual comparisons of the maturity of ICT related processes and security technologies. The reviews are conducted in the context of on-site inspections at the largest banks. The differences are evaluated and supervisory tools used for low performance entities. The supervisory expectations with regards to ICT security controls are strengthened according to the evolution of the cyber threat landscape. Developments at institutions are monitored on a regular basis accordingly to ensure ICT security controls and mitigations are still effective in view of the evolution of the cyber threat landscape. At the CA side the onsite inspection methodology covers the institutions' protection against advanced cyber threats (table-top cyber-exercise).

125. CAs were asked if they face challenges in assessing the controls to mitigate material ICT risks, applying the criteria set out in paragraph 46 of the Guidelines. Several CAs (10) faced such challenges.

126. The challenges faced by CAs in assessing the controls to mitigate material ICT risks include the following:

- Lack of information provided by institutions
- Complexity of the landscape
- Supervisors with specialized ICT skills required for assessment of controls, typically through on-site missions or deep dives

[17] EBA/GL/2019/04

[18] EBA/GL/2019/02

- Institutions' policy frameworks being not sufficiently up-to-date, consistent and clear
- Lack of an adequate and sufficiently documented framework for managing ICT risks
- Insufficient resources or expertise at institutions for appropriate management of security-related risks
- No regular testing of ICT security and ICT continuity plans
- Outsourcing and third-party policy frameworks insufficiently covering controls to mitigate ICT outsourcing risks
- Insufficient internal audit coverage of security and IT continuity risks

127. Most CAs (28) apply the sub-categories of ICT risks set out in paragraph 52 of the Guidelines when assessing ICT risk controls that are specific for the identified material risks. One CA is planning to do so. Two CAs do not apply the sub-categories of ICT risks set out in the Guidelines for this assessment.

128. Some CAs (8) apply guidance beyond the criteria set out in the Guidelines when assessing ICT risk controls that are specific for the identified material risks. One CA is planning to do so.

129. If CAs use additional criteria for the assessment of the controls to mitigate material ICT risks, those are mostly set out in the national regulatory frameworks. Reference is also made to the EBA Guidelines on ICT and Security Risk management,[19] to the SSM SREP methodology for LSIs, to the EBA Guidelines on outsourcing arrangements,[20] to international standards (COBIT, ISO), and the BCBS 239 principles for effective risk data aggregation and risk reporting.

130. CAs were asked if they face challenges in assessing the sub-categories of ICT risks set out in paragraph 52 of the Guidelines. Several CAs (13) faced such challenges.

131. The challenges faced by CAs in assessing the sub-categories of ICT risks set out in paragraph 52 of the Guidelines include the following:

- Lack of information from institutions on the different sub-categories of ICT risk (e.g. proper recognition of outsourced activities)
- Difficulties to properly assess the sub-categories of ICT risk off-site (e.g. ICT availability and continuity risks, ICT change risks, ICT data integrity risks) so assessment of some of the risks in the SREP relies mainly on latest on-site inspections

[19] EBA/GL/2019/04

[20] EBA/GL/2019/02

- Lack of supervisors with specialized ICT skills needed for the assessment
- Lack of international benchmarks for quantitative indicators
- Overlaps and dependencies between sub-categories of ICT risks (e.g. for ICT outsourcing risk)
- Assessment of the quality of implementation of security tools and related processes in ICT security risk, which is a growing challenge due to increasing cyber-threats
- Assessment of the long-term projects to comply with BCBS 239 and their impact on ICT data integrity risk

132. Three CAs apply approaches different from the guidance set out in paragraphs 53 to 60 of the Guidelines for the assessment of the sub-categories of ICT risks and specific controls. One CA assesses the sub-categories of ICT risks and specific controls against the controls articulated in the EBA Guidelines on ICT and Security Risk Management[21] - Sections 3.4, 3.6 and 3.7 - and against the EBA Guidelines on outsourcing arrangements[22] for the sub-category of ICT outsourcing risks. The additional criteria used include:

(i) additional categories of IT Governance, Internal Revision and IT risk management in risk controls;

(ii) additional questions regarding the IT strategy, IT organizational documents, IT budget, definition of responsibilities and segregation of duties, available IT resources and IT reporting in IT Governance;

(iii) assessment of risk controls for non-material risks in case IT risk management is assessed as unsatisfactory.

Another CA uses a process and methodology which cover all the sub-categories as set out in the Guidelines though organized in a different manner making it difficult to match with the sub-categories set out in the Guidelines on a one-to-one basis.

133. CAs were asked if the guidance for the assessment of controls for material ICT risks as set out in paragraph 52 of the Guidelines should be further elaborated. Two CAs indicated the guidance should be further elaborated. In particular, the guidance for the ICT data integrity risks should be further elaborated. And for all of the ICT risk sub-categories set out in paragraph 52, the guidance should be updated with respect to the EBA Guidelines on ICT and security risk management, the EBA Guidelines on outsourcing arrangements, and the upcoming DORA.

[21] EBA/GL/2019/04

[22] EBA/GL/2019/02

d. Assessment of ICT security risk exposures and controls

134. CAs were asked for how many of the institutions under their supervision they assessed (in compliance with the Guidelines) the institutions' ICT security risk exposures as material in the last two years.

- 15 CAs assessed ICT security risk exposures as material for more than 75% of the institutions
- 7 CAs assessed ICT security risk exposures as material for 50% to 75% of the institutions
- 9 CAs assessed ICT security risk exposures as material for less than 50% of the institutions

135. Most CAs (26) that identified deficiencies in the ICT security risk controls submitted findings and/or recommendations to the credit institutions. Two CAs did not yet submit such findings and/or recommendations but are planning to do so. Three CAs did not submit such findings and/or recommendations.

136. Most CAs (27) apply the guidance set out in paragraph 55 of the Guidelines for assessing the ICT security risk controls. Three CAs are planning to do so.

137. CAs were asked which inputs they use to assess the institutions' ICT security risk controls. The inputs are ranked by number of CAs indicating to use them as input for the assessment of the institutions' ICT security risk controls for all institutions.

- Cyber security incident reporting to the CA (used for all institutions by 26 CAs)
- Assessment of institution's ICT security policy (used for all institutions by 25 CAs)
- Assessment of institution's ICT security risk framework (used for all institutions by 24 CAs)
- Assessment of institution's security incident management and escalation process (used for all institutions by 24 CAs)
- Assessment of institutions' measures/controls to protect the ICT systems from attacks from the internet or other external networks (used for all institutions by 23 CAs)
- Assessment of institutions' ICT security risk awareness and information campaigns (used for all institutions by 20 CAs)
- Assessment of institutions' security penetration testing (used for all institutions by 20 CAs)
- Assessment of physical security measures (used for all institutions by 18 CAs)

- Assessment of institutions' user and administrative activity logging (used for all institutions by 17 CAs)
- Security penetration testing by external parties (third parties, TIBER, or other) (used for all institutions by 16 CAs)

138. Other inputs used for the assessment of the institutions' ICT security risk controls include:

- ICT self-assessment questionnaires
- Internal and external audit reports
- Thematic reviews
- On-site inspections (including at ICT service providers)
- Reporting under PSD2 (major incident reporting, annual report on operational and ICT security risk)
- Unavailability or security incidents reported to the CA
- Annual IT reports under the local regulatory reporting framework
- Major IT project monitoring documents
- Other external sources when available (including TIBER-EU exercises or providers of ratings and other indicators regarding the level of information security risk of institutions' internet facing IT systems).

139. Just over half of the responding CAs (17) have a methodology to rate, measure and benchmark ICT security risks and controls at institutions. Several CAs (9) are planning to have such methodology, one of them is being implemented for the 2022 SREP cycle. 5 CAs do not have such a methodology.

140. Several of the methodologies used to rate, measure and benchmark ICT security risks and controls involve self-assessment questionnaires on the level of risks and controls that are completed by the institutions, and assessed, scored and benchmarked by CAs.

Annex 1. Compliance table of the Guidelines

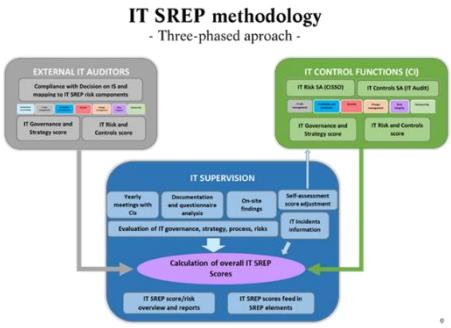
EBA/GL/2017/05 Appendix 1
11 May 2017; Date of application – 01 January 2018 (Updated – 21 September 2022)

Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)

The following competent authorities* comply or intend to comply with the EBA's Guidelines on ICT Risk Assessment under SREP:

		Competent authority	Complies or intends to comply	Comments
Member State				
BE	Belgium	National Bank of Belgium	**Yes**	As at 05.02.2019, notification date. As of January 2018, the National Bank of Belgium is compliant with the Guidelines on ICT Risk Assessment under the SREP (EBA/GL/2017/OS), in the sense that for every financial institution that undergoes a Supervisory Review and Evaluation Process, an ICT risk assessment is made according to these guidelines. The implementation for Significant Institutions is fully aligned with the ECB-SSM processes/instructions in this regard, and also for Less Significant Institutions the NBB intends to align its implementation to the finalized instructions of the ECB-SSM when available.
BG	Bulgaria	Българска народна банка (Bulgarian National Bank)	**Yes**	As at 20.09.2019, notification date. In accordance with Article 74a of the Law on Credit Institutions banks shall apply the EBA guidelines, recommendations concerning them and for which the BNB has announced it shall comply with in accordance with Article 79a, paragraph 1, item 2 of the same Law.

		Competent authority	Complies or intends to comply	Comments
				The EBA/GL/2017/05 is part of the legal framework to the BNB Manual for the SREP (adopted by Decision Nr 279/14.11.2018 of the BNB Governing Council); Under the Manual, the supervisory assessment of bank's ICT risk is accomplished in the course of the assessment of the operational risk, as well as in the context of the risk management framework. The SREP Manual is available only in Bulgarian language.
CZ	Czech Republic	Czech National Bank	**Yes**	As at 03.11.2017, notification date.
DK	Denmark	Finanstilsynet (FSA-DK)	**Yes**	Complies as of the date of the notification, 20.09.2022. The Danish FSA has been compliant with "EBA/GL/2017/05 – GLs on ICT Risk Assessment under the Supervisory Review Process (SREP)" since the "intention to comply" date (01.01.2020). For further information please refer to the peer review report by the Peer Review Committee.
DE	Germany	Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)	**Yes**	As at 01.01.2019, notification date.
EE	Estonia	Finantsinspektsioon	**Yes**	As at 01.11.2017 notification date
IE	Ireland	Central Bank of Ireland	**Yes**	As at 04.02.2019, notification date.
EL	Greece	Bank of Greece	**Yes**	Complies as of date of notification, 20/07/2022. Executive Committee Act 190/16.6.2021 Bank of Greece Circular 33/17.1.2022
HR	Croatia	Hrvatska narodna banka (Croatian National Bank)	**Yes**	As at 02.10.2010, notification date. In line with requirements stemming from EBA Guidelines on ICT Risk Assessment under SREP (EBA/GL/2017/05), CNB developed and implemented its own IT risk methodology under SREP. Methodology and CNB's approach were presented at EBA Workshop on IT risk supervision and cloud outsourcing (December 2017). IT risk assessment includes assessment of the institution's governance and strategy on ICT (feeds into the assessment of

		Competent authority	Complies or intends to comply	Comments
				internal governance and institution-wide controls) and assessment of institutions' ICT risk exposures and controls (contributes to the assessment of Operational risk as a part of risks to capital). Information for the assessments is collected from multiple sources (external IT auditors, internal IT control and IT management functions of credit institutions etc.) and by using various techniques (questionnaires, self-assessments, reports, documents analysis and yearly meetings). A brief overview of the methodology is shown in the next diagram:-  By using this methodology, in 2018. CNB performed IT risk assessment for SREP I (OSI), SREP II and SREP III categories of credit institutions. IT SREP scores were included into overall SREP scores. ~~As at 28.01.2019, notification date.~~ ~~In line with requirements stemming from EBA Guidelines on ICT Risk Assessment under SREP (EBA/GL/2017/05), CNB developed and implemented its own IT risk methodology under SREP. Methodology and CNB's approach was presented at EBA Workshop on IT risk supervision and cloud outsourcing (December 2017.).~~ ~~IT risk assessment includes assessment of the institution's governance and strategy on ICT (feeds into the assessment of internal governance and institution-wide controls) and assessment of institution's ICT risk exposures and controls (contributes to the assessment of Operational risk as a~~

		Competent authority	Complies or intends to comply	Comments
				~~part of risks to capital). Information for the assessments is collected from multiple sources (external IT auditors, internal IT control and IT management functions of credit institutions etc.) and by using various techniques (questionnaires, self-assessments, reports, documents analysis and yearly meetings). By using this methodology, in 2018. CNB did IT risk assessment for SREP I (OSI), SREP II and SREP III categories of credit institutions. IT SREP scores were included into overall SREP scores.~~
ES	Spain	Banco de España	**Yes**	As at 07.02.2019, notification date.
FR	France	Autorité de Contrôle Prudentiel et de Résolution (ACPR)	**Yes**	As at 21.02.2019, notification date. ACPR has complied through an internal document.
IT	Italy	Banca d'Italia	**Yes**	As at 03.05.2019, notification date.
CY	Cyprus	Central Bank of Cyprus	**Yes**	As at 22.04.2019, notification date.
LV	Latvia	Financial and Capital Market Commission	**Yes**	As at 01.02.2019, notification date. EBA Guidelines are directly applicable by the FCMC during the SREP Assessment process.
LT	Lithuania	Bank of Lithuania	**Yes**	As at 04.02.2019, notification date. Compliance with GL approved by the Supervision Services Decision no 241-33.
LU	Luxembourg	Commission de Surveillance du Secteur Financier (CSSF)	**Yes**	As at 05.02.2019, notification date.
HU	Hungary	The Central Bank of Hungary	**Yes**	As at 22.02.2019, notification date. Implementing document: ICAAP-ILAAP-BMA Methodological Handbook of the MNB (https://www.mnb.hu/felugyelet/szabalyozas/felugyeleti-szabalyozo-eszkozok/modszertani-kezikonyvek/icaap-ilaap-bma-felugyeleti-felulvizsgalatok).
MT	Malta	Malta Financial Services Authority	**Yes**	As at 04.02.2019, notification date.

		Competent authority	Complies or intends to comply	Comments
NL	Netherlands	De Nederlandsche Bank	**Yes**	As at 10.11.2017, notification date.
AT	Austria	Austrian Financial Market Authority	**Yes**	As at 07.11.2017, notification date
PL	Poland	Komisja Nadzoru Finansowego	**Yes**	As at 15.02.2019, notification date.
PT	Portugal	Banco de Portugal	**Yes**	As at 05.02.2019, notification date.
RO	Romania	National Bank of Romania	**Yes**	As at 10.11.2017, notification date.
SI	Slovenia	Bank of Slovenia	**Yes**	As at 01.01.2018, notification date. https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2017-01-3103?so=2017-01-3103
SK	Slovakia	Národná Banka Slovenska	**Yes**	Complies as of the date of the notification, 15.07.2022. EBA GL is already fully implemented in NBS supervisory processes.
FI	Finland	Finanssivalvonta (FIN-FSA)	**Yes**	As at 15.02.2018, notification date.
SE	Sweden	Finansinspektionen	**Yes**	As at 30.01.2019, notification date.
UK	United Kingdom	PRA	**Yes**	As at 05.03.2018, notification date.
		Financial Conduct Authority	**Yes**	As at 09.02.2019, notification date.

EU Institutions – Agencies

ECB	ECB	ECB	**Yes**	As at 05.02.2019, notification date.

EEA – EFTA State

IS	Iceland	Financial Supervisory Authority, Iceland	**Yes**	As at 10.11.2017, notification date

		Competent authority	Complies or intends to comply	Comments
LI	Liechtenstein	Financial Market Authority Liechtenstein (FMA)	**Yes**	As at 10.11.2017, notification date
NO	Norway	The Financial Supervisory Authority of Norway	**Yes**	As at 04.02.2019, notification date.
		European Territories under Article 355(3) TFEU		
UK	United Kingdom	Gibraltar Financial Services Commission	**Yes**	As at 04.02.2019, notification date.

*The EEA States other than the Member States of the European Union are not currently required to notify their compliance with the EBA's Guidelines. This table is based on information provided from those EEA States on a voluntary basis.

** Please note that, in the interest of transparency, if a competent authority continues to intend to comply after the application date, it will be considered "non-compliant" unless (A) the Guidelines relate to a type of institution or instruments which do not currently exist in the jurisdiction concerned; or (B) legislative or regulatory proceedings have been initiated to bring any national measures necessary to comply with the Guidelines in force in the jurisdiction concerned.

Notes

Article 16(3) of the EBA's Regulations requires national competent authorities to inform us whether they comply or intend to comply with each Guideline or recommendation we issue. If a competent authority does not comply or does not intend to comply it must inform us of the reasons. We decide on a case by case basis whether to publish reasons.

The EBA endeavour to ensure the accuracy of this document, however, the information is provided by the competent authorities and, as such, the EBA cannot accept responsibility for its contents or any reliance placed on it.

For further information on the current position of any competent authority, please contact that competent authority. Contact details can be obtained from the EBA's website www.eba.europa.eu.

Annex 2. Country codes and acronyms of relevant competent authorities

Country Code	Country	Competent Authority
AT	Austria	Finanzmarktaufsicht (Financial Market Authority)
BE	Belgium	National Bank of Belgium (NBB)
BG	Bulgaria	Българска народна банка (Bulgarian National Bank)
CY	Cyprus	Κεντρική Τράπεζα της Κύπρου (Central Bank of Cyprus)
CZ	Czech Republic	Ceska Narodni Banka (Czech National Bank (CNB))
DE	Germany	Bundesanstalt für Finanzdienstleistungsaufsicht (Federal Financial Supervisory Authority, BaFin)
DK	Denmark	Finanstilsynet (Danish Financial Supervisory Authority (Danish FSA))
ECB-SSM		European Central Bank – Single Supervisory Mechanism
EE	Estonia	Finantsinspektsioon (Estonian Financial Supervision and Resolution Authority)
ES	Spain	Banco de España (Bank of Spain)
FI	Finland	Finanssivalvonta (Finnish Financial Supervisory Authority)
FR	France	Autorité de Contrôle Prudentiel et de Résolution (Prudential Supervisory & Resolution Authority (ACPR))
GR	Greece	Τράπεζα της Ελλάδος (Bank of Greece)
HR	Croatia	Hrvatska Narodna Banka (Croatian National Bank)
HU	Hungary	Magyar Nemzeti Bank (The Central Bank of Hungary)
IS	Iceland	Fjármálaeftirlitið (Icelandic Financial Supervisory Authority (FME))
IE	Ireland	Central Bank of Ireland
IT	Italy	Banca d'Italia (Bank of Italy)
LI	Liechtenstein	Finanzmarktaufsicht – FMA (Financial Market Authority)
LT	Lithuania	Lietuvos Bankas (Bank of Lithuania)
LU	Luxembourg	Commission de Surveillance du Secteur Financier (Commission for the Supervision of the Financial Sector (CSSF))
LV	Latvia	Finansu un Kapitala Tirgus Komisija (Financial and Capital Market Commission)
MT	Malta	Malta Financial Services Authority (MFSA)

Country Code	Country	Competent Authority
NL	Netherlands	De Nederlandsche Bank (Dutch Central Bank (DNB))
NO	Norway	Finanstilsynet (Norwegian Financial Supervisory Authority)
PL	Poland	Komisja Nadzoru Finansowego (Polish Financial Supervision Authority (KNF))
PT	Portugal	Banco de Portugal (Bank of Portugal)
RO	Romania	Banca Naţională a României (National Bank of Romania)
SE	Sweden	Finansinspektionen (Swedish Financial Supervisory Authority)
SI	Slovenia	Banka Slovenije (Bank of Slovenia)
SK	Slovakia	Narodna Banka Slovenska (National Bank of Slovakia)

Annex 3. Summary of CAs responses to benchmark questions

	Incorporation Guidelines into the SREP methodology	Dedicated methodology for ICT risk assessment	Methodology to assign an ICT risk score based on the Guidelines	List of ICT risk sub-categories and risk scenarios in Annex of Guidelines used
Country Code	Q1	Q2	Q5	Q20
AT	yes-fully	yes-fully	not yet, but planning	yes-partially
BE	yes-fully	yes-fully	yes-fully	yes-fully
BG	yes-partially	yes-partially	no	not yet, but planning
CY	yes-fully	yes-fully	no	yes-partially
CZ	yes-fully	yes-fully	yes-fully	yes-fully
DE	yes-fully	yes-fully	yes-fully	yes-fully
DK	yes-partially	yes-fully	yes-fully	yes-partially
ECB-SSM	yes-fully	yes-fully	yes-fully	yes-fully
EE	yes-fully	yes-fully	yes-fully	yes-fully
ES	yes-fully	yes-fully	yes-fully	yes-partially
FI	yes-partially	yes-partially	no	yes-partially
FR	yes-fully	yes-fully	yes-partially	not yet, but planning
GR	yes-fully	yes-fully	yes-fully	yes-fully
HR	yes-fully	yes-fully	yes-fully	yes-fully
HU	yes-partially	no	yes-partially	yes-partially
IE	yes-fully	yes-fully	yes-fully	yes-fully
IS	yes-partially	yes-partially	non-contributing	yes-partially
IT	yes-fully	yes-fully	yes-partially	yes-fully
LI	yes-fully	yes-partially	yes-partially	not yet, but planning
LT	yes-partially	yes-partially	not yet, but planning	yes-partially
LU	yes-fully	yes-fully	yes-partially	yes-partially
LV	yes-fully	yes-fully	yes-fully	yes-fully
MT	yes-partially	yes-partially	yes-partially	yes-partially
NL	yes-fully	yes-fully	yes-partially	yes-partially
NO	yes-partially	yes-partially	yes-partially	yes-fully
PL	yes-fully	yes-fully	yes-partially	yes-fully
PT	yes-fully	yes-fully	yes-fully	yes-fully
RO	yes-fully	yes-partially	yes-partially	yes-fully
SE	yes-partially	yes-fully	yes-fully	no
SI	yes-fully	yes-fully	no	yes-partially
SK	yes-fully	yes-fully	yes-fully	yes-fully

Annex 4. Self-Assessment Questionnaire for CAs

Implementation of the EBA Guidelines on ICT Risk Assessment under SREP, EBA/GL/2017/05 ('the Guidelines')

General implementation of the Guidelines

1. Have you incorporated the Guidelines into the SREP methodology? [yes-fully/ yes-partially/ not yet, but planning/ no]

2. Have you set up a dedicated methodology for ICT risk assessment (in or outside the SREP methodology)? [yes-fully/ yes-partially/ not yet, but planning/ no]

3. How do you incorporate proportionality for ICT risk in your methodology? (such as ICT risk profiles, business models, type of activities, SREP categorization, other) [Comment box]

4. How do you incorporate your assessment of ICT risks in the SREP assessment of business model, of governance and risk management, and of operational risk? [Comment box]

5. Have you set up a methodology to assign an ICT risk score based on the Table 1 of the Guidelines? [yes-fully/ yes-partially/ not yet, but planning/ no]

- If so, please indicate the relevant criteria. [Comment box]

6. How do you consider the score you determine for ICT risks when assigning the score for operational risk? [Comment box]

7. In your assessment of the ICT risk under SREP, do you use inputs from third parties, such as auditors, for certain provisions of the guidelines? [yes/ not yet, but planning/ no] [comment box]

8. Which inputs do you use in your assessment of the ICT risk under SREP from other supervisory processes/tools [on-site inspections, off-site work, outcomes of self-assessment questionnaires, cyber incident reporting, threat-led penetration tests (e.g. TIBER) other [Comment box]]?

- How do you use these inputs [Comment box]

9. What are the main three challenges (ranked by importance) you face for the assessment of the ICT risk under SREP under the GLs (practical, organizational, or other) and how do you address these challenges? [1.[Comment box], 2.[Comment box], 3.[Comment box]]

10. Do you perform horizontal analysis on the ICT risk assessment under SREP? [yes/ no]

- If so, please describe the analysis. [Comment box]

Supervisory practices in ICT Risk Assessment under SREP

General supervision, prioritisation and resources

11. How do you see the importance of the supervision of ICT risk in your jurisdiction considering risk-based approach to allocation of supervisory resources? [Very important, Important, Somewhat important, Not important]

12. According to the supervisory priorities defined in your Competent Authority, is the total number of resources for ICT risks supervision (horizontal and off/on-site) considered [Adequate, mostly adequate, not adequate with improvements needed]

- If not adequate, what additional resource(s) does your competent authority seek? With what expertise/specialist skills? [Comment box]

- If not adequate, what difficulties do you face for hiring staff with adequate expertise/specialist skills? [Comment box]

13. How do you improve levels of expertise and skills in general supervisory staff in your competent authority? [internal training, external training, SSM training, inclusion of general staff in ICT risk supervisory work/on-site inspections, other [Comment box]]

14. If ICT training is provided to general supervisory staff, please indicate if you have a training curriculum, the number of training sessions in 2021 provided in total, and the number of trained supervisors in 2021 [Comment box]

15. How do you see the importance of the supervision of ICT risk in your jurisdiction in terms of supervisory priorities (based on your CA's work programme and identified priorities) for the last two years? [High, medium, or low priority]

16. Do you take any specific initiatives to support the incorporation of the ICT risk assessment in SREP? If yes, please indicate which one(s):

- ○ ICT related training provided to supervisory staff
- ○ Use of IT solutions to facilitate the assessment process
- ○ Use of a dedicated methodology to facilitate the assessment process
- ○ Monitoring of ICT risk related metrics or key indicators
- ○ Other [Comment box]

Assessment of materiality of ICT risk and ICT risk taxonomy

17. Have you set out criteria for considering ICT risk as material, beyond those criteria already set out in paragraph 17 (criteria specified in Section 6.1) of the Guidelines? [yes/ not yet, but planning/ no]

- If so, what criteria are used, how they are applied and how do they influence the ICT risk assessment under SREP? [Comment box]

18. For how many of the institutions you supervise do you consider ICT risk as material (applying the criteria set out in paragraph 17 of the GLs and/or additional criteria)?

- ○ For less than 33% of the institutions supervised ICT risk is considered as material
- ○ For 33% to 66% of the institutions supervised ICT risk is considered as material
- ○ For more than 66% of the institutions supervised ICT risk is considered as material

19. For how many of the institutions for which you consider ICT risk as material (applying the criteria set out in paragraph 17 of the GLs and/or additional criteria) do you score ICT risk as an individual sub-category of operational risk?

- ○ For less than 33% of the institutions supervised for which ICT risk is considered as material, ICT risk is scored as an individual sub-category of operational risk
- ○ For 33% to 66% of the institutions supervised for which ICT risk is considered as material, ICT risk is scored as an individual sub-category of operational risk

- For most more than 66% of the institutions supervised for which ICT risk is considered as material, ICT risk is scored as an individual sub-category of operational risk

20. Do you use the list of ICT risk sub-categories and risk scenarios set out in the Annex of the Guidelines)? [yes-fully/ yes-partially/ not yet, but planning/ no] [Comment box]

- If so, have you set out any additional risk sub-categories and risk scenarios? [Comment box]
- If so, should some ICT risk sub-categories and risk scenarios in the Guidelines be considered for deletion or improvement? [Comment box]
- Follow up question for ECB: Are there any country-specific differences, please explain [Comment box]

Supervisory practices

21. For how many institutions you supervise have you assessed ICT risk in compliance with the GLs in the last two-years?

- For less than 50% of institutions
- For 50% to 75% of the institutions
- For more than 75% of the institutions

[comment box]

ICT strategies

22. For how many of the institutions you supervise have you assessed (in compliance with the GLs) the adequacy, the development and the implementation of ICT strategies defined by credit institutions in the last two-years?

- For none or less than 50% of the institutions
- For 50% to 75% of the institutions
- For more than 75% of the institutions

- Have you identified shortcomings/deficiencies with regards to the ICT strategy? [Yes/ No]
- Where relevant deficiencies in the ICT strategy framework and implementation have been identified, have you submitted findings or recommendations to credit institutions? [Yes/ No/ not yet, but planning]
- Have you applied the guidance referred to in section 2.2 of the Guidelines in your assessment of the ICT strategy (including its adequacy, its development and its implementation)? [Yes/ No/ not yet, but planning]
- Have you applied guidance, beyond those provisions already set out in the Guidelines? [yes/ not yet, but planning/ no]
- If so, what additional criteria are used and how are they applied? [Comment box]

23. Are you performing regular oversight of the implementation of the ICT strategies by credit institutions? [Yes/ No/ not yet, but planning]

- If so, what challenges do you see for institutions in the implementation of ICT strategies? [Legacy systems, Lack of skills/expertise, Dependencies from third parties (outsourcing), Integration issues from mergers and acquisitions, Other [Comment box]]

ICT internal governance

24. For how many of the institutions you supervise have you reviewed institutions' ICT internal governance in compliance with the GLs in the last two years?

- For less than 50% institutions
- For 50% to 75% of the institutions
- For more than 75% the institutions

- Have you applied the guidance referred to in section 2.3 of the Guidelines in your assessment of the ICT internal governance? [Yes/ No/ not yet, but planning]
- Have you applied guidance, beyond those provisions already set out in the Guidelines? [yes/ not yet, but planning/ no]

- If so, what additional criteria are used and how they are applied? [Comment box]

- Where any deficiencies in ICT internal governance have been identified, have you submitted findings or recommendations to credit institutions? [Yes/ No/ not yet, but planning]

ICT risk management framework

25. For how many of the institutions you supervise have you assessed institutions' ICT risk management framework in compliance with the GLs in the last two years?

  - For less than 50% of the institutions
  - For 50% to 75% of the institutions
  - For more than 75% of the institutions

- Have you applied the guidance referred to in section 2.4 of the Guidelines in your assessment of the ICT risk management framework? [Yes/ No/ not yet, but planning]

- Have you applied guidance, beyond those provisions already set out in the Guidelines? [yes/ not yet, but planning/ no]

- If so, what additional criteria are used and how they are applied? [Comment box]

- Where any deficiencies in ICT risk management framework have been identified, have you submitted findings or recommendations to credit institutions? [Yes/ No/ not yet, but planning]

26. Do you conduct the assessment under point (a) of paragraph 31 of the Guidelines having regard to both expected and adverse scenarios, e.g. scenarios included in the institution-specific or supervisory stress test as set in paragraph 31 of the Guidelines? [Yes/ No].

- If so, which scenarios where considered? [Comment box]

- If supervisory stress tests were used, please describe these [Comment box]

ICT risk exposures and controls

27. For how many of the institutions you supervise have you assessed institutions' ICT risk exposures and controls in compliance with the GLs in the last two years?

- ○ For less than 50% of the institutions
- ○ For 50% to 75% of the institutions
- ○ For more than 75% of the institutions

- Have you applied the guidance referred to in section 3 of the Guidelines in your assessment of ICT risk exposures and controls? [Yes/ No/ not yet, but planning]
- Where any deficiencies in ICT controls have been identified, have you submitted findings or recommendations to credit institutions? [Yes/ No/ not yet, but planning]

28. Have you assessed (in compliance with the GLs) the methodology and the processes applied by the institutions to identify the ICT systems and services that are critical? [Yes/ No/ not yet, but planning]

- Have you applied guidance, beyond those provisions already set out in the Guidelines? [yes/ not yet, but planning/ no]
- If so, what additional criteria are used and how they are applied? [Comment box]
- Do you face challenges in assessing the criticality of the ICT systems and services? [Yes/No]
- If so, what are these challenges [Comment box]

29. When identifying material ICT risks (section 3.2 of the Guidelines), do you apply the criteria set out in the Guidelines? [Yes/ No/ not yet, but planning]

- Have you applied guidance, beyond those provisions already set out in the Guidelines? [yes/not yet, but planning/ no]
- If so, what additional criteria are used and how they are applied? [Comment box]
- Do you face challenges in assessing the materiality of ICT risks? [Yes/No]
- If yes, what type of challenges (comment box)

30. When assessing the controls to mitigate material ICT risks (section 3.3 of the Guidelines), do you apply the criteria set out in paragraph 46 the Guidelines? [Yes/ No/ not yet, but planning]

- Have you applied guidance, beyond those provisions already set out in the Guidelines? [yes/ not yet, but planning/ no]
- If so, what additional criteria are used and how they are applied? [Comment box]
- Do you face challenges in applying the criteria set out in paragraph 46 the Guidelines (assessing the controls to mitigate material ICT risks)? [Yes/No]
- If so, what are these challenges [Comment box]

31. When assessing ICT risk controls that are specific for the identified material risks (section 3.3.4 of the Guidelines), do you apply the sub-categories of ICT risks set out in paragraph 52 of the Guidelines? [Yes/ No/ not yet, but planning]

- Have you applied guidance, beyond those criteria already set out in these paragraphs of the Guidelines? [yes/not yet, but planning/ no]
- If so, what additional criteria are used and how they are applied and why? [Comment box]
- Do you face challenges in assessing the sub-categories of ICT risks set out in paragraph 52 the Guidelines? [Yes/No]
    - ICT availability and continuity risks [Yes/No]
    - ICT security risks [Yes/No]
    - ICT change risks [Yes/No]
    - ICT risk data integrity risks [Yes/No]
    - ICT outsourcing risks [Yes/No]
- If so, what are these challenges [Comment box]
- In the assessment of the sub-categories of ICT risks and specific controls when material risks have been identified in such sub-categories, as set out in paragraph 52 the Guidelines, do

you apply approaches that are different from the guidance set in paragraphs 53 to 60 of the Guidelines? [Yes/No]

- ICT availability and continuity risks [Yes/No]
  - If so, what is the approach? [Comment box]
- ICT security risks [Yes/No]
  - If so, what is the approach? [Comment box]
- ICT change risks [Yes/No]
  - If so, what is the approach? [Comment box]
- ICT risk data integrity risks [Yes/No]
  - If so, what is the approach? [Comment box]
- ICT outsourcing risks [Yes/No]
  - If so, what is the approach? [Comment box]
- Other sub-category of ICT risks [Yes/No]
  - If so, what is the approach? [Comment box]

- Do you think the assessment guidance for the criteria set out in paragraph 52 of the guidance should be further elaborated? [Yes/No]
  - If so, what elements guidance are missing?
    - ICT availability and continuity risks [Comment box]
    - ICT security risks [Comment box]
    - ICT change risk [Comment box]
    - ICT data integrity risks [Comment box]
    - ICT outsourcing risks [Comment box]

ICT security risk exposures and controls (Section 3.3.4.b of the Guidelines)

32. For how many of the institutions you supervise have you assessed (in compliance with the Guidelines) the institutions' ICT security risk exposures as material in the last two years?

- ○ For less than 50% of the institutions
- ○ For 50% to 75% of the institutions
- ○ For more than 75% of the institutions

- Have you applied the guidance referred to in paragraph 55 (section 3.3.4 (b)) of the Guidelines in your assessment of ICT security risk controls? [Yes/ No/ not yet, but planning]
- Where any deficiencies in ICT security risk controls have been identified, have you submitted findings or recommendations to credit institutions? [Yes/ No/ not yet, but planning]

33. Which inputs do you use to assess the institutions' ICT security risk controls?

- Assessment of institutions' security risk framework
  - ○ All institutions
  - ○ Part of the institutions
  - ○ None of the institutions
- Assessment of institutions' ICT security policy
  - ○ All institutions
  - ○ Part of the institutions
  - ○ None of the institutions
- Assessment of institutions' security incident management and escalation process
  - ○ All institutions
  - ○ Part of the institutions

- None of the institutions

- Assessment of institutions' user and administrative activity logging
  - All institutions
  - Part of the institutions
  - None of the institutions
- Assessment of institutions' ICT security risk awareness and information campaigns
  - All institutions
  - Part of the institutions
  - None of the institutions
- Assessment of physical security measures [if so, onsite/off-site]
  - All institutions
  - Part of the institutions
  - None of the institutions
- Assessment of institutions' measures to protect the ICT systems from attacks from the internet (i.e. cyber-attacks) or other external networks
  - All institutions
  - Part of the institutions
  - None of the institutions
- Assessment of institutions' security penetration testing
  - All institutions
  - Part of the institutions

- None of the institutions

- Security penetration testing by external parties (third parties, TIBER, other)
  - All institutions
  - Part of the institutions
  - None of the institutions
- Cyber security incident reporting to the competent authority
  - All institutions
  - Part of the institutions
  - None of the institutions
- Other inputs used [Comment box]
- Comments [Comment box]

- Do you have a methodology to rate, measure and benchmark ICT security risk and controls at institutions? [Yes/ No/ not yet, but planning] [Comment box]

General comments or remarks on the Guidelines

34. Please provide any additional comments or suggestions you might have with regards to the Guidelines [Comment box]

EUROPEAN BANKING AUTHORITY

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