EBA/GL/2017/05

11 May 2017

Final Report

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

Contents

1. Executive Summary

These Guidelines are addressed to competent authorities and are intended to promote common procedures and methodologies for the assessment of the Information and Communication Technology (ICT) risk under the supervisory review and evaluation process (SREP), referred to in Article 97 of Directive 2013/36/EU[1]. In particular, these Guidelines drawn up pursuant to Article 107(3) of Directive 2013/36/EU, supplement and further specify criteria for the assessment of ICT risk as part of operational risk put forward in the EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP)[2] (from here on 'EBA SREP Guidelines'). These Guidelines form an integral part of the EBA SREP Guidelines and should be read and applied along with it.

These Guidelines set out the requirements competent authorities should apply in their assessment of ICT focusing on the general provisions and application of scoring as part of the SREP assessment of risks to capital (Title 1), assessment of institutions' governance and strategy on ICT (Title 2); and assessment of institutions' ICT risk exposures and controls (Title 3).

In particular, Title 1 of these Guidelines explains how the assessment of ICT risk contributes to the overall SREP assessment of an institution, noting that the assessment of ICT risk would contribute (1) to the assessment of operational risk, which is assessed as part of the assessment of risks to capital (Title 6 of the EBA SREP Guidelines), (2) the assessment of institutions' governance and strategy on ICT would feed into the assessment of internal governance and institution-wide controls under Title 5 of the EBA SREP Guidelines, and (3) the assessment of all aspects of ICT covered by these Guidelines would also inform the business model analysis performed in accordance with Title 4 of the EBA SREP Guidelines.

It is noted that whilst generally competent authorities would assess sub-categories of risks as part of the main categories (i.e. ICT risk will be assessed as part of operational risk), where competent authorities deem some categories material, they may assess such sub-categories on an individual basis. To this end, where ICT risk is identified as a material risk by the competent authority, these Guidelines also provide a scoring table 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 EBA SREP Guidelines.

Title 2, on the assessment of the institution's governance and strategy on ICT covers how the institution's overall internal governance and institution wide controls address ICT specifically ensuring adequate knowledge and understanding at the management body level, as well as assessing the institution's ICT strategy from the perspective of both the governance of the ICT strategy and its alignment with, and impact on, the institution's business model. The assessment of the alignment between the ICT strategy and the business strategy is included in these Guidelines because of the strong links between the two.

[1] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (1) - OJ L 176, 27.6.2013.

[2] EBA/GL/2014/13.

The assessment of ICT risk and the controls in place as a 'risk to capital' under Title 3 broadly follows the same structure of the EBA SREP Guidelines assessment of operational risk in that it starts by assessing the risk exposure, then the effectiveness of controls in order to complete the assessment and to be able to feed into the findings and score of operational risk where ICT risk was already included in the EBA SREP Guidelines (Table 6 of the EBA SREP Guidelines).

When applying these Guidelines competent authorities should consider the principle of proportionality, in particular the depth and detail of the ICT risk assessment should be proportionate to the size, structure and operational environment of the institution as well as the nature, scale and complexity of its activities.

These Guidelines are complemented by an ICT risk taxonomy in the annex which includes ICT risk categories specified in these Guidelines with a non-exhaustive list of examples of material ICT risks which competent authorities should reflect on as part of the assessment under Title 3 of these Guidelines.

The EBA has held a public consultation on these Guidelines, and the text has been amended to reflect the outcomes of the consultation. The detailed analysis of the feedback received and the EBA response is provided in this final report.

Next steps

The Guidelines will be translated into the official EU languages and published on the EBA website. The deadline for competent authorities to report whether they comply with the Guidelines will be two months after the publication of the translations. The Guidelines will apply from 1 January 2018.

2. Background and rationale

Information and communication technology (ICT) play and important role in the functioning of institutions, and the risks associated with ICT may pose significant prudential impact and even threaten the viability of an institution. Under the current EBA SREP Guidelines competent authorities are required to assess ICT risk as a sub-category of operational risk and the EBA SREP Guidelines provide broad criteria that competent authorities should consider in their assessments.

ICT, using the terminology from the EBA SREP Guidelines but also more commonly known as IT (Information Technology), is a key resource in developing and supporting banking services; ICT systems are not only key enablers of institutions' strategies, forming the backbone of almost all banking processes and distribution channels, but they also support the automated controls environment on which core banking data is based. ICT systems and services also represent material proportions of institutions' costs, investments and intangible assets. Furthermore, technological innovation plays a crucial role in the banking sector from a strategic standpoint, as a source of competitive advantage, as it is a fundamental tool to compete in the financial market with new products as well as through facilitating the restructuring and optimisation of the value chain. As a result of the increasing importance of ICT in the banking industry, some recent trends include:

a. the emergence of (new) cyber risks together with the increased potential for cybercrime and the appearance of cyber terrorism; and

b. the increasing reliance on outsourced ICT services and third party products, often in the form of diverse packaged solutions resulting in manifold dependencies and potential constraints and new concentration risks.

In view of the growing importance and increasing complexity of ICT risk within the banking industry and in individual institutions, the EBA has developed this additional guidance to assist the competent authorities in their assessment of ICT risk as part of the SREP.

These Guidelines build on existing references to ICT risk in the SREP Guidelines and also feed into the SREP methodology more generally, whilst setting out the requirements competent authorities should apply in their assessment of ICT focusing on the general provisions and application of scoring as part of the SREP assessment of risks to capital (Title 1), assessment of institutions' governance and strategy on ICT (Title 2); and assessment of institutions' ICT risk exposures and controls (Title 3).

Acknowledging the growing importance of ICT systems and hence the increasing potential prudential impact from their failures on an institution and on the sector as a whole (in particular due to interlinkages between the institutions also in the cross-border context), and taking into account the technical specificities of ICT risk assessments and the objective to increase convergence of supervisory practices in the ICT supervisory risks assessments within the EEA, these Guidelines provide guidance to supervisors for assessing ICT risk in institutions.

Competent authorities should perform the assessment of ICT risk and the governance arrangement and ICT strategy as part of the SREP process following the minimum engagement model and proportionality criteria specified in Title 2 of the EBA SREP Guidelines. In particular, this means that:

a. the frequency of the ICT risk assessment would depend on the minimum engagement model driven by the SREP category an institution is assigned to and its specific supervisory examination programme; and

b. the depth, detail and intensity of the ICT assessment should be proportionate to the size, structure and operational environment of the institution as well as the nature, scale and complexity of its activities.

These Guidelines mainly feed into and complement the existing ICT risk assessment component of the EBA SREP Guidelines, under operational risk (Section 6.4). Recognising the need for ICT to also be taken into account in an institution's internal governance and institution-wide controls, these Guidelines additionally include references to what competent authorities should assess with regard to management of ICT risks at senior management level and management body level. This feeds into the assessment of an institution's internal governance and institution-wide controls as specified in Title 5 of the EBA SREP Guidelines. Furthermore, these Guidelines also include guidance on the assessment of an institution's ICT strategy and the alignment with the institution's business strategy which should inform institutions' the business model analysis performed in accordance with Title 4 of the EBA SREP Guidelines.

These Guidelines are aimed at addressing risks arising to market integrity and the viability of institutions from ICT. The Guidelines do not therefore explicitly address ICT risks arising to consumers, although the EBA would expect that beneficial effects will materialise indirectly, as a result of the comprehensive assessment of ICT risks as set out in the Guidelines.

The focus of these Guidelines is on the ICT dimensions of the risk management processes covered in these Guidelines and not the business aspects.

Like the EBA SREP Guidelines, these Guidelines do not specify whether onsite or offsite inspections are most appropriate to conduct the assessments contained within these Guidelines. This is left to competent authorities to decide what is the most efficient and effective manner to be able to complete the assessment for each institution taking into account the need for proportionality and allowing for discretion and judgment of the competent authorities given the specific features of national banking systems.

These Guidelines do not introduce additional reporting obligations and assume that the assessments specified in the Guidelines are made on the basis of information already being collected or readily available information at the institution to which the competent authority has an easy and sufficient access, and/or already collected information by the competent authority in accordance with the Commission

Implementing Regulation (EU) No 680/2014 on supervisory reporting[3]. However, where necessary, competent authorities should be able to request additional information from the institution.

[3] Commission Implementing Regulation (EU) No 680/2014_of 16 April 2014 laying down implementing technical standards with regard to supervisory reporting of institutions according to Regulation (EU) No 575/2013 of the European Parliament and of the Council Text with EEA relevance.

3. Guidelines

EBA/GL/2017/05

Guidelines

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

1. Compliance and reporting obligations

Status of these Guidelines

1. This document contains Guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010[4]. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with the Guidelines.

2. Guidelines set the EBA view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 to whom Guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where Guidelines are directed primarily at institutions.

Reporting requirements

3. According to Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA as to whether they comply or intend to comply with these Guidelines, or otherwise with reasons for non-compliance, by ([dd.mm.yyyy]). In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website to compliance@eba.europa.eu with the reference 'EBA/GL/2017/05. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to EBA.

4. Notifications will be published on the EBA website, in line with Article 16(3).

[4] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC, (OJ L 331, 15.12.2010, p.12).

2. Subject matter, scope and definitions

Subject matter and scope of application

5. These Guidelines, drawn up pursuant to Article 107(3) of Directive 2013/36/EU[5] aim to ensure the convergence of supervisory practices in the assessment of the information and communication technology (ICT) risk under the supervisory review and evaluation process (SREP) referred to in Article 97 of Directive 2013/36/EU and further specified in the EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP)[6]. In particular these Guidelines specify the assessment criteria that competent authorities should apply in the supervisory assessment of institutions' governance and strategy on ICT and the supervisory assessment of institutions' ICT risk exposures and controls. These Guidelines form an integral part of the EBA SREP Guidelines.

6. Competent authorities should apply these Guidelines in line with the level of application of SREP specified in the EBA SREP Guidelines and in accordance with the minimum engagement model and proportionality requirements established therein.

Addressees

7. These Guidelines are addressed to competent authorities as defined in point (i) of Article 4(2) of Regulation (EU) No 1093/2010.

Definitions

8. Unless otherwise specified, terms used and defined in Directive 2013/36/EU, Regulation (EU) No 575/2013 and definitions from the EBA SREP Guidelines have the same meaning in these Guidelines. In addition, for the purposes of these Guidelines, the following definitions apply:

ICT systems	ICT set-up as part of a mechanism or an interconnecting network that support the operations of an institution.
ICT services	Services provided by ICT systems to one or more internal or external users. Examples include data entry, data storage, data

[5] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (1) - OJ L 176, 27.6.2013.

[6] EBA/GL/2014/13

	processing and reporting services, but also monitoring, business and decision support services.
ICT availability and continuity risk	The risk that performance and availability of ICT systems and data are adversely impacted, including the inability to timely recover the institution's services, due to a failure of ICT hardware or software components; weaknesses in ICT system management; or any other event, as further elaborated in the Annex.
ICT security risk	The risk of unauthorised access to ICT systems and data from within or outside the institution (e.g. cyber-attacks), as further elaborated in the Annex.
ICT change risk	The risk arising from the inability of the institution to manage ICT system changes in a timely and controlled manner, in particular for large and complex change programmes, as further elaborated in the Annex.
ICT data integrity risk	The risk that data stored and processed by ICT systems are incomplete, inaccurate or inconsistent across different ICT systems, for example as a result of weak or absent ICT controls during the different phases of the ICT data life cycle (i.e. designing the data architecture, building the data model and/or data dictionaries, verifying data inputs, controlling data extractions, transfers and processing, including rendered data outputs), impairing the ability of an institution to provide services and produce (risk) management and financial information in a correct and timely manner, as further elaborated in the Annex.
ICT outsourcing risk	The risk that engaging a third party, or another Group entity (intra-group outsourcing), to provide ICT systems or related services adversely impacts the institution's performance and risk management, as further elaborated in the Annex.

3. Implementation

Date of application

9. These Guidelines apply from 1 January 2018.

4. Requirements for the ICT Risk Assessment

Title 1 - General provisions

10. Competent authorities should perform the assessment of ICT risk and the governance arrangement and ICT strategy as part of the SREP process following the minimum engagement model and proportionality criteria specified in Title 2 of the EBA SREP Guidelines. In particular, this means that:

    a. the frequency of the ICT risk assessment would depend on the minimum engagement model driven by the SREP category an institution is assigned to and its specific supervisory examination programme; and

    b. the depth, detail and intensity of ICT assessment should be proportionate to the size, structure and operational environment of the institution as well as the nature, scale and complexity of its activities.

11. The principle of proportionality applies throughout these Guidelines to the scope, frequency and intensity of supervisory engagement and dialogue with an institution and supervisory expectations of the standards the institution should meet.

12. Competent authorities may rely on and take into consideration work already undertaken by the institution or by the competent authority in the context of the assessments of other risks or SREP elements in order to have an update of the assessment. Specifically, in conducting the assessments specified in these Guidelines competent authorities should select the most appropriate supervisory assessment approach and methodology that is best suited and proportionate to the institution and competent authorities should use existing and available documentation (e.g. relevant reports and other documents, meetings with (risk) management, on-site inspection findings) to inform the competent authorities' assessment.

13. Competent authorities should summarise the findings of their assessments of the criteria specified in these Guidelines and use them for the purposes of reaching conclusions on the assessment of the SREP elements as specified in the EBA SREP Guidelines.

14. In particular, the assessment of governance and ICT strategy performed in accordance with Title 2 of these Guidelines should result in findings that inform the summary of findings of the assessment of internal governance and institution-wide controls element of SREP as specified in Title 5 of the EBA SREP Guidelines and be reflected the respective scoring of that SREP element. Furthermore, competent authorities should consider that any significant adverse impact of the ICT strategy assessment on the institution's business strategy or any concerns that the institution may not have sufficient ICT resources

and ICT capabilities to perform and support important planned strategic changes should inform the business model analysis performed in accordance with Title 4 of the EBA SREP Guidelines.

15. The outcome of the assessment of ICT risk as specified in Title 3 of these Guidelines should inform the findings of the assessment of operational risk and should be considered as informing the relevant score as specified in in Title 6.4 of the EBA SREP Guidelines.

16. It is noted that whilst generally competent authorities should assess sub-categories of risks as part of the main categories (i.e. ICT risk will be assessed as part of operational risk), where competent authorities 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 competent authority, these 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 EBA SREP Guidelines.

17. To reach a view on whether ICT risk should be considered as material and therefore the possibility for ICT risk to be assessed and scored as an individual sub-category of operational risk, competent authorities may use the criteria specified in Section 6.1 of the EBA SREP Guidelines.

18. When applying these Guidelines competent authorities should, where relevant, consider the non-exhaustive list of ICT risk sub-categories and risk scenarios as set out in the Annex, noting that the Annex focusses on ICT risks that may result in high severity losses. Competent authorities may exclude some of the ICT risks included in the taxonomy if not pertinent to their assessment. Institutions are expected to maintain their own risk taxonomies rather than using the ICT risk taxonomy set out in the Annex.

19. Where these Guidelines are applied in relation to cross-border banking groups and their entities, and a college of supervisors has been established, competent authorities involved should, in the context of their cooperation for the SREP assessment in accordance with Section 11.1 of the EBA SREP Guidelines, coordinate to the maximum extent possible the exact and detailed scope of each information item consistently for all group entities.

Title 2 - Assessment of institutions' governance and strategy on ICT

2.1 General principles

20. Competent authorities should assess whether the institution's general governance and internal control framework duly cover the ICT systems and related risks and if the management body adequately addresses and manages these aspects, as ICT is integral to the proper functioning of an institution.

21. In conducting this assessment, competent authorities should refer to the requirements and standards of good internal governance and risk control arrangements as specified in the EBA Guidelines on Internal Governance (GL 44)[7] and international guidance in this field to the extent these are applicable given the specificity of ICT systems and risks.

22. The assessment in this Title does not cover the specific elements of the ICT system governance, risk management and controls that are focused on managing specific ICT risks addressed under Title 3 of these Guidelines, but focuses on the following areas:

    a. ICT strategy - whether the institution has an ICT strategy that is adequately governed and is in line with the institution's business strategy;

    b. overall internal governance– whether the institution's overall internal governance arrangements are adequate in relation to the institution's ICT systems; and

    c. ICT risk in the institution's Risk management framework –whether the institution's risk management and internal control framework adequately safeguards the institution's ICT systems.

23. Point a) referred to in paragraph 22, while providing information about elements of the institution's governance, should mainly feed into the assessment of the business model addressed under Title 4 of the EBA SREP Guidelines. Points b) and c) further complement assessments of topics covered by Title 5 of the EBA SREP Guidelines and the assessment described in these Guidelines should feed into the respective assessment under Title 5 of the EBA SREP Guidelines.

24. The outcome of this assessment should inform, where relevant, the assessment of risk management and controls in Title 3 of these Guidelines.

2.2 ICT strategy

25. Under this section competent authorities should assess whether the institution has an ICT strategy in place: that is subject to adequate oversight from the institution's management body; that is consistent

[7] EBA Guidelines on Internal Governance, GL 44, 27 September 2011.

with the business strategy, particularly for keeping its ICT up-to-date and planning or implementing important and complex ICT changes; and that supports the institution's business model.

2.2.1 ICT strategy development and adequacy

26. Competent authorities should assess whether the institution has a framework in place, proportionate to the nature, scale and complexity of its ICT activities, for the preparation and development of the institution's ICT strategy. In conducting this assessment competent authorities should take into account whether:

    a. the senior management[8] of the business line(s) is adequately involved in the definition of the institution's strategic ICT priorities and that, in turn, senior management of the ICT function is aware of the development, design and initiation of major business strategies and initiatives to ensure the continued alignment between ICT systems, ICT services and the ICT function (i.e. those responsible for the management and deployment of these systems and services), and the institution's business strategy, and that ICT are effectively up-dated;

    b. the ICT strategy is documented and supported by concrete implementation plans, in particular regarding the important milestones and resource planning (including financial and human resources) to ensure that they are realistic and enable the delivery of the ICT strategy;

    c. the institution periodically updates its ICT strategy, in particular when changing the business strategy, to ensure continued alignment between the ICT and business medium-term to long-term objectives, plans and activities; and

    d. the institution's management body approves the ICT strategy, implementation plans and monitors its implementation.

2.2.2 ICT strategy implementation

27. If the institution's ICT strategy requires the implementation of important and complex ICT changes, or changes with material implications for the institution's business model, competent authorities should assess whether the institution has a control framework in place, appropriate to its size, its ICT activities as well as the level of change activities, to support the effective implementation of the institution's ICT strategy. In conducting this assessment competent authorities should take into account whether the control framework:

    a. includes governance processes (e.g. progress and budget monitoring and reporting) and relevant bodies (e.g. a project management office (PMO), an ICT steering group or equivalent) to effectively support the implementation of the ICT strategic programmes;

    b. has defined and allocated the roles and responsibilities for the implementation of ICT strategic programmes, paying particular attention to the experience of key stakeholders in organising, steering and monitoring important and complex ICT changes and the

[8] Senior management and management body as defined in the Directive 2013/36/EU of 26 June 2013 in Article 3 (7) 'management body', and Article 3 (9) 'senior management'.

management of the wider organisational and human impacts (e.g. managing resistance to change, training, communication).

c. engages the independent control and internal audit functions to provide assurance that the risks associated with ICT strategy implementation have been identified, assessed and effectively mitigated and that the governance framework in place to implement the ICT strategy is effective; and

d. contains a planning and planning review process that provides flexibility to respond to important identified issues (e.g. encountered implementation problems or delays) or external developments (e.g. important changes in the business environment, technological issues or innovations) to ensure a timely adaptation of the strategic implementation plan.

2.3 Overall internal governance

28. In accordance with Title 5 of the EBA SREP Guidelines, competent authorities should assess whether the institution has an appropriate and transparent corporate structure that is 'fit for purpose', and has implemented appropriate governance arrangements. With specific regard to ICT systems and in line with the EBA Guidelines on internal governance, this assessment should include an assessment of whether the institution demonstrates:

a. a robust and transparent organisational structure with clear responsibilities on ICT, including the management body and its committees and that key responsible persons for ICT (e.g. chief information officer 'CIO', chief operating officer 'COO' or equivalent role) have adequate indirect or direct access to the management body, to ensure that important ICT-related information or issues are adequately reported, discussed and decided upon at the level of the management body; and

b. that the management body knows and addresses the risks associated with the ICT;

29. Further to section 5.2 of the EBA SREP Guidelines, competent authorities should assess whether the institution's ICT outsourcing policy and strategy considers, where relevant, the impact of ICT outsourcing on the institution's business and business model.

2.4 ICT risk in the institution's risk management framework

30. In assessing the institution's institution-wide risk management and internal controls, as provided by Title 5 of the EBA SREP Guidelines, competent authorities should consider whether the institution's risk management and internal control framework adequately safeguards the institution's ICT systems in a way which is commensurate to the size and activities of the institution and its ICT risk profile as defined in Title 3. In particular, competent authorities should determine whether:

a. the risk appetite and the ICAAP cover the ICT risks, as part of the broader operational risk category, for the definition of the overall risk strategy and determination of internal capital; and

b. the ICT risks are within the scope of institution-wide risk management and internal control frameworks.

31. Competent authorities should conduct the assessment under point (a) above having regard to both expected and adverse scenarios, e.g. scenarios included in the institution-specific or supervisory stress test.

32. With specific regard to b), competent authorities should assess whether the independent control and internal audit functions, as detailed in paragraphs 104 (a), 104 (d), 105 (a) and 105 (c) of the EBA SREP Guidelines, are appropriate to ensure a sufficient level of independence between the ICT and the control and audit functions, given the size and ICT risk profile of the institution.

2.5 Summary of findings

33. These results should be reflected in the summary of findings under Title 5 of the EBA SREP Guidelines and should form part of the respective scoring in line with the considerations in Table 3 of the EBA SREP Guidelines.

34. For the assessment of ICT strategy, the following points should be considered in concluding the above assessment:

a. if competent authorities come to the conclusion that the institution's governance framework is inadequate for developing and implementing the institution's ICT strategy under 2.2 then this should inform the assessment of the institution's internal governance in Title 5 of the EBA SREP Guidelines under point 87 (a);

b. if competent authorities come to the conclusion from the above assessments under 2.2 that there would be a significant misalignment between the ICT strategy and the business strategy that may have a significant adverse impact of the institution's long term business and/or financial objectives, the institution's sustainability and/or business model, or the institution's business areas/lines which have been determined as most material in paragraph 62 (a) of the EBA SREP Guidelines, then this should inform the business model assessment of Title 4 of the SREP GL under points 70 (b) and 70 (c); and

c. if competent authorities come to the conclusion from the above assessments under 2.2 that the institution may not have sufficient ICT resources and ICT implementation capabilities to perform and support important planned strategic changes this should inform the business model assessment of Title 4 of the EBA SREP Guidelines under point 70 (b).

Title 3 - Assessment of institutions' ICT risks exposures and controls

3.1 General considerations

35. Competent authorities should assess whether the institution has properly identified, assessed and mitigated its ICT risks. This process should be part of the operational risk management framework and congruent to the approach applying to operational risk.

36. Competent authorities should first identify the material inherent ICT risks to which the institution is or might be exposed, followed by an assessment of the effectiveness of the institution's ICT risks' management framework, procedures and controls to mitigate these risks. The outcome of the assessment should be reflected in a summary of findings which feeds into the operational risk score in the SREP Guidelines. Where ICT risk is deemed to be material and competent authorities want to assign an individual score then Table 1 should be used to assign a score as a sub-risk of operational risk.

37. When performing the assessment under this Title, competent authorities should use all available information sources as set out in paragraph 127 of Title 6 of the EBA SREP Guidelines e.g. institution's risk management activities, reporting and outcomes, as a basis for the identification of their supervisory assessment priorities. Competent authorities should also use other sources of information to conduct this assessment, including the following where relevant:

    a. ICT risk and controls self-assessments (if provided in the ICAAP information);
    b. ICT risk related Management Information (MI) submitted to the institution's management body, e.g. periodic and incident driven ICT risk reporting (including in the operational loss database), ICT risk exposure data from the institution's risk management function;
    c. ICT related internal and external audit findings reported to the institution's audit committee.

3.2 Identification of material ICT risks

38. Competent authorities should identify the material ICT risks to which the institution is or might be exposed following the steps below.

3.2.1 Review of the institution's ICT risk profile

39. When reviewing the institution's ICT risk profile, competent authorities should consider all relevant information about the institution's ICT risk exposures, including the information under paragraph 37 and the identified material deficiencies or weaknesses in the ICT organisation and institution –wide controls under Title 2 of these Guidelines, and where relevant review this information in a proportionate manner. As part of this review, competent authorities should consider:

a. the potential impact of a significant disruption on the institution's ICT systems on the financial system either at domestic or international level;
b. whether the institution may be subject to ICT security risks or ICT availability and continuity risks due to internet dependencies, high adoption of innovative ICT solutions or other business distribution channels that may make it a more likely target for cyber-attacks;
c. whether the institution may be more exposed to ICT security risks, ICT availability and continuity risks, ICT data integrity risks or ICT change risks due to the complexity (e.g. as a result of mergers or acquisitions) or outdated nature of its ICT systems;
d. whether the institution is implementing material changes to its ICT systems and/or ICT function (e.g. as a result of mergers, acquisitions, divestments or the replacement of its core ICT systems), which may adversely impact the stability or orderly functioning of the ICT systems and can result in material ICT availability and continuity risks, ICT security risks, ICT change risks or ICT data integrity risks;
e. whether the institution has outsourced ICT services or ICT systems within or outside the group that may expose it to material ICT outsourcing risks;
f. whether the institution is implementing aggressive ICT cost cutting measures which may lead to the reduction of needed ICT investments, resources and IT expertise and can increase the exposure to all the ICT risks types in the taxonomy;
g. whether the location of important ICT operations/data centres (e.g. regions, countries) may expose the institution to natural disasters (e.g. flooding, earthquakes), political instability or labour conflicts and civil disturbances which can lead to a material increase of ICT availability and continuity risks and ICT security risks.

3.2.2 Review of the critical ICT systems and services

40. As part of the process to identify the ICT risks with a potential significant prudential impact on the institution, competent authorities should review documentation from the institution and form an opinion on which ICT systems and services are critical for the adequate functioning, availability, continuity and security of the institution's essential activities.

41. To this end, competent authorities should review the methodology and processes applied by the institution to identify the ICT systems and services that are critical, taking into consideration that some ICT systems and services may be considered critical by the institution from a business continuity and availability perspective, a security (e.g. fraud prevention) and/or a confidentiality perspective (e.g. confidential data). When performing the review, competent authorities should conduct their review taking into consideration that critical ICT systems and services should fulfil at least one of the following conditions:

a. they support the core business operations and distribution channels (e.g. ATMs, internet and mobile banking) of the institution;
b. they support essential governance processes and corporate functions, including risk management (e.g. risk management and treasury management systems);
c. they fall under special legal or regulatory requirements (if any) that impose heightened availability, resilience, confidentiality or security requirements (e.g. data protection legislation

or possible 'Recovery Time Objectives' (RTO, the maximum time within which a system or process must be restored after an incident) and 'Recovery Point Objective' (RPO, the maximum time period during which data can be lost in case of an incident)) for some systemically important services (if and where applicable));

d. they process or store confidential or sensitive data to which unauthorised access could significantly impact the institution's reputation, financial results or the soundness and continuity of its business (e.g. databases with sensitive customer data); and/or

e. they provide base line functionalities that are vital for the adequate functioning of the institution (e.g. telecom and connectivity services, ICT and cyber security services).

3.2.3 Identification of material ICT risks to critical ICT Systems and Services

42. Taking into account the performed reviews of the institution's ICT risk profile and critical ICT systems and services above, competent authorities should form an opinion on the material ICT risks that, in their supervisory judgement, can have a significant prudential impact on the institution's critical ICT systems and services.

43. When assessing the potential impact of ICT risks on the critical ICT systems and services of an institution, competent authorities should consider:

a. The financial impact, including (but not limited to) loss of funds or assets, potential customer compensation, legal and remediation costs, contractual damages, lost revenue;

b. The potential for business disruption, considering (but not limited to) the criticality of the financial services affected; the number of customers and/or branches and employees potentially affected;

c. The potential reputational impact on the institution based on the criticality of the banking service or operational activity affected (e.g. theft of customer data); the external profile/visibility of the ICT systems and services affected (e.g. mobile or on-line banking systems, point of sale, ATMs or payment systems);

d. The regulatory impact, including the potential for public censure by the regulator, fines or even variation of permissions.

e. The strategic impact on the institution, for example if strategic product or business plans are compromised or stolen.

44. Competent authorities should then map the identified ICT risks that are considered material into the following ICT risk categories for which additional risk descriptions and examples are provided in the Annex. Competent authorities should reflect on the ICT risks in the Annex as part of the assessment under Title 3:

a. ICT availability and continuity risk
b. ICT security risk
c. ICT change risk
d. ICT data integrity risk

e. ICT outsourcing risk

The mapping is to assist competent authorities in determining which risks are material (if any) and therefore should be subject to a closer and/or deeper review in the following assessment steps.

3.3 Assessment of the controls to mitigate material ICT risks

45. To assess the institution's residual ICT risk exposure, competent authorities should review how the institution identifies, monitors, assesses and mitigates the material risks identified by the competent authorities in the assessment above.

46. To this end, for the identified material ICT risks, competent authorities should review the applicable:

a. ICT risk management policy, processes and risk tolerance thresholds;

b. Organisational management and oversight framework;

c. Internal audit coverage and findings; and

d. ICT risk controls that are specific for the identified material ICT risk.

47. The assessment should take into account the outcome of the analysis of the overall risk management and internal control framework as referred to in Title 5 of the EBA SREP Guidelines, as well as the institution's governance and strategy addressed in Title 2 of these Guidelines, as significant deficiencies identified in these areas may influence the ability of the institution to manage and mitigate its ICT risk exposures. Where relevant, competent authorities should also make use of information sources in paragraph 37 of these Guidelines.

48. Competent authorities should perform the following assessment steps in a manner that is proportionate to the nature, scale and complexity of the institution's activities and by applying a supervisory review that is appropriate to the institution's ICT risk profile.

3.3.1 ICT risk management policy, processes and tolerance thresholds

49. Competent authorities should review whether the institution has appropriate risk management policies, processes and tolerance thresholds in place for the identified material ICT risks. These can be a part of the operational risk management framework or a separate document. For this assessment competent authorities should take into account whether:

a. the risk management policy is formalised and approved by the management body and contains sufficient guidance on the institution's ICT risk appetite, and on the main pursued ICT risk management objectives and/or applied ICT risk tolerance thresholds. The relevant ICT risk management policy should also be communicated to all relevant stakeholders;

b. the applicable policy covers all significant elements for the risk management of the identified material ICT risks;

c. the institution has implemented a process and underlying procedures for the identification (e.g. 'risk control self-assessments' (RCSA), risk scenario analysis) and monitoring of the involved material ICT risks; and
d. the institution has an ICT risk management reporting in place that provides timely information to senior management and the management body, and which allows senior management and/or the management body to assess and monitor whether the institution´s ICT risk mitigation plans and measures are consistent with the approved risk appetite and/or tolerance thresholds (where relevant) and to monitor changes of material ICT risks.

3.3.2 Organisational management and oversight framework

50. Competent authorities should assess how the applicable risk management roles and responsibilities are embedded and integrated in the internal organisation to manage and oversee the identified material ICT risks. In this regard competent authorities should assess whether the institution demonstrates:

a. clear roles and responsibilities for the identification, assessment, monitoring, mitigation, reporting and oversight of the involved material ICT risk;
b. that the risk responsibilities and roles are clearly communicated, allocated and embedded in all relevant parts (e.g. business lines, IT) and processes of the organisation, including the roles and responsibilities for gathering and aggregating the risk information and reporting it to senior management and/or the management body;
c. that the ICT risk management activities are performed with sufficient and qualitatively appropriate human and technical resources. To assess the credibility of the applicable risk mitigation plans, competent authorities should also assess whether the institution has allocated sufficient financial budgets and/or other required resources for their implementation;
d. an adequate follow-up and response of the management body regarding important findings from the independent control functions regarding the ICT risk(s), taking into account the possible delegation of some aspects to a committee, where this exists; and
e. that exceptions from applicable ICT regulations and policies are recorded and subject to a documented review and reporting by the independent control function with a focus on the related risks.

3.3.3 Internal audit coverage and findings

51. Competent authorities should consider whether the Internal Audit Function is effective with regards to auditing the applicable ICT risk control framework, by reviewing whether:

a. the ICT risk control framework is audited with the required quality, depth and frequency and commensurate with the size, activities and the ICT risk profile of the institution;
b. the audit plan includes audits on the critical ICT risks identified by the institution;
c. the important ICT audit findings, including agreed actions, are reported to the management body; and

d. ICT audit findings, including agreed actions, are followed up and progress reports periodically reviewed by the senior management and/or the audit committee.

3.3.4 ICT risk controls that are specific for the identified material ICT risks

52. For the identified material ICT risks, competent authorities should assess whether the institution has specific controls in place to address these risks. The following sections provide a non-exhaustive list of the specific controls to be considered when assessing the material risks identified under point 3.2.3 that were mapped to the following ICT risk categories:

a. ICT availability and continuity risks;
b. ICT security risks;
c. ICT change risks;
d. ICT data integrity risks;
e. ICT outsourcing risks.

(a) Controls for managing material ICT availability and continuity risks

53. In addition to the requirements in the EBA SREP Guidelines (para 279 - 281) competent authorities should assess whether the institution has an appropriate framework in place for identifying, understanding, measuring and mitigating ICT availability and continuity risks.

54. For this assessment, competent authorities should, in particular, take into account whether the framework:

a. identifies the critical ICT processes and the relevant supporting ICT systems that should be part of the business resilience and continuity plans with:

i. a comprehensive analysis of dependencies between the critical business processes and supporting systems;

ii. determination of recovery objectives for the supporting ICT systems (e.g. typically determined by the business and/or regulations in terms of RTO and RPO);

iii. appropriate contingency planning to enable the availability, continuity, and recovery of critical ICT systems and services to minimize disruption to an institution's operations within acceptable limits.

b. has business resilience, continuity control environment policies and standards and operational controls which include:

i. Measures to avoid that a single scenario, incident or disaster might impact both ICT production and recovery systems;

ii. ICT system backup and recovery procedures for critical software and data, that ensure that these backups are stored in a secure and sufficiently remote location, so that an incident or disaster cannot destroy or corrupt these critical data;

iii. monitoring solutions for the timely detection of ICT availability or continuity incidents;

iv. a documented incident management and escalation process, that also provides guidance on the different incident management and escalation roles and responsibilities, the members of the crisis committee(s) and the chain of command in case of emergency;

v. physical measures to both protect the institution's critical ICT infrastructure (e.g. data centres) from environmental risks (e.g. flooding and other natural disasters) and ensure an appropriate operating environment for ICT systems (e.g. air conditioning);

vi. processes, roles and responsibilities to ensure that also outsourced ICT systems and services are covered by adequate business resilience and continuity solutions and plans;

vii. ICT performance and capacity planning and monitoring solutions for critical ICT systems and services with defined availability requirements, to detect important performance and capacity constraints in a timely manner;

viii. solutions to protect critical internet activities or services (e.g. e-banking services), where necessary and appropriate, against denial of service and other cyber-attacks from the internet, aimed at preventing or disturbing access to these activities and services.

c. tests ICT availability and continuity solutions, against a range of realistic scenarios including cyber-attacks, fail-over tests and tests of back-ups for critical software and data which:

i. are planned, formalised and documented, and the test results used to strengthen the effectiveness of the ICT availability and continuity solutions;

ii. include stakeholders and functions within the organisation, such as business line management including business continuity, incident and crisis response teams, as well as relevant external stakeholders in the ecosystem;

iii. management body and senior management are appropriately involved in (e.g. as part of crisis management teams) and are informed of test results.

(b) Controls for managing material ICT security risks

55. Competent authorities should assess whether the institution has an effective framework in place for identifying, understanding, measuring and mitigating ICT security risk. For this assessment competent authorities should, in particular, take into account whether the framework considers:

a. clearly defined roles and responsibilities regarding:

i. the person(s) and/or committees that are responsible and/or accountable for the day to day ICT security management and the elaboration of the overarching ICT security policies, with attention for their needed independence;

ii. the design, implementation, management and monitoring of ICT security controls;

iii. the protection of critical ICT systems and services by adopting for example a vulnerability assessment process, software patch management, end point protection (e.g. malware virus), Intrusion detection and prevention tools;

iv. the monitoring, classification and handling of external or internal ICT security incidents; including incident response and the resumption and recovery of the ICT systems and services;
v. regular and proactive threat assessments to maintain appropriate security controls.

b. an ICT security policy that takes into consideration and, where appropriate, adheres to internationally recognised ICT security standards and security principles (e.g. the 'principle of least privilege' i.e. limiting access to the minimal level that will allow normal functioning for access right management and the principle of "defence in depth" i.e. layered security mechanisms increase security of the system as a whole for designing a security architecture);

c. a process to identify ICT systems, services and commensurate security requirements reflecting potential fraud risk and/or possible misuses and/or abuses of confidential data along with documented security expectations to be adhered to for these identified ICT systems, services and data, aligned with the institution's risk tolerance and monitored for their correct implementation;

d. a documented security incident management and escalation process, that provides guidance on the different incident management and escalation roles and responsibilities, the members of the crisis committee(s) and the chain of command in case of security emergencies;

e. user and administrative activity logging to enable effective monitoring and the timely detection and response to unauthorised activity; to assist in or to conduct forensic investigations of security incidents. The institution should have in place logging policies that define appropriate types of logs to be maintained and their retention period;

f. awareness and information campaigns or initiatives to inform all levels in the institution on the safe use and protection of the institution's ICT systems and the main ICT security (and other) risks they should be aware of, in particular regarding the existing and evolving cyber threats (e.g. computer viruses, possible internal or external abuses or attacks, cyber-attacks) and their role in mitigating security breaches;

g. adequate physical security measures (e.g. CCTV, burglar alarm, security doors) to prevent unauthorised physical access to critical and sensitive ICT systems (e.g. data centres);

h. measures to protect the ICT systems from attacks from the Internet (i.e. cyber-attacks) or other external networks (e.g. traditional telecom connections or connections with trusted partners). Competent authorities should review whether the institution's framework considers:

i. a process and solutions to maintain a complete and up to date inventory and overview of all the outward facing network connection points (e.g. websites, internet applications, WIFI, remote access) through which third parties could break into the internal ICT systems.

ii. closely managed and monitored security measures (e.g. firewalls, proxy servers, mail relays, antivirus and content scanners) to secure the incoming and outgoing network traffic (e.g. e-mail) and the outward facing network connections through which third parties could break into the internal ICT systems;

iii. processes and solutions to secure websites and applications that can be directly attacked from the internet and/or the outside, that can serve as an entry point into the internal ICT systems. In general these include a combination of recognised secure development practices, ICT system hardening and vulnerability scanning practices, and/or the

implementation of additional security solutions like for example application firewalls and/or intrusion detection (IDS) and/or intrusion prevention (IPS) systems;

iv. periodic security penetration testing to assess the effectiveness of implemented cyber and internal ICT security measures and processes. These tests should be performed by staff and/or external experts with the necessary expertise, with documented test results and conclusions reported to senior management and/or the management body. Where needed and applicable, the institution should learn from these tests where to further improve the security controls and processes and/or to obtain better assurance on their effectiveness.

(c) Controls for managing material ICT change risks

56. Competent authorities should assess whether the institution has an effective framework in place for identifying, understanding, measuring and mitigating ICT change risk commensurate with the nature, scale and complexity of the institution's activities and the ICT risk profile of the institution. The institution's framework should cover the risks associated with the development, testing and approval of ICT systems changes, including the development or change of software, before they are migrated to the production environment and ensure an adequate ICT lifecycle management. For this assessment competent authorities should, in particular, take into account whether the framework considers:

a. documented processes for managing and controlling changes to ICT systems (e.g. configuration and patch management) and data (e.g. bug fixing or data corrections), ensuring the adequate involvement of ICT risk management for important ICT changes that may significantly impact the institution's risk profile or exposure;

b. specifications regarding the required segregation of duties during the different phases of the implemented ICT change processes (e.g. solution design and development, testing and approval of new software and/or changes, migration and implementation in the production environment, and bug fixing), with a focus on the implemented solutions and segregation of duties to manage and control changes to the production ICT systems and data by ICT staff (e.g. developers, ICT system administrators, data base administrators) or any other party (e.g. business users, service providers);

c. test environments that adequately reflect production environments;

d. an asset inventory of the existing applications and ICT systems in the production environment, as well as the test and development environment, so that required changes (e.g. version updates or upgrades, systems patching, configuration changes) can be properly managed, implemented and monitored for the involved ICT systems.

e. a process to monitor and manage the life cycle of the used ICT systems, to ensure that they continue to meet and support the actual business and risk management requirements and to make sure that the used ICT solutions and systems are still supported by their vendors; and that this is accompanied by adequate software development life cycle (SDLC) procedures.

f. a software source code control system and appropriate procedures to prevent unauthorised changes in the source code of software that is developed in-house;

g. a process to conduct a security and vulnerability screening of new or materially modified ICT systems and software, before releasing them into production and exposing them to possible cyber-attacks;

h. a process and solutions to prevent the unauthorised or unintended disclosure of confidential data, when replacing, archiving, discarding or destroying ICT systems;

i. an independent review and validation processes to reduce the risks for human errors when performing changes to the ICT systems that may have an important adverse effect on the availability, continuity or security of the institution (e.g. important changes to the firewall configuration), or security of the institution (e.g. changes to the firewalls).

(d) Controls for managing material ICT data integrity risks

57. Competent authorities should assess whether the institution has an effective framework in place for identifying understanding, measuring and mitigating ICT data integrity risk commensurate with the nature, scale and complexity of the institution's activities and the ICT risk profile of the institution. The institution's framework should consider the risks associated with preserving the integrity of the data stored and processed by the ICT systems. For this assessment, competent authorities should, in particular take into account whether the framework considers:

a. a policy that defines the roles and responsibilities for managing the integrity of the data in the ICT systems (e.g. data architect, data officers[9], data custodians[10], data owners/stewards[11]) and provides guidance on which data are critical from a data integrity perspective and should be subject to specific ICT controls (e.g. automated input validation controls, data transfer controls, reconciliations, etc.) or reviews (e.g. a compatibility check with the data architecture) in the different phases of ICT data life cycle;

b. a documented data architecture, data model and/or dictionary, that is validated with relevant business and IT stakeholders to support the needed data consistency across the ICT systems and to make sure that the data architecture, data model and/or dictionary remain aligned with business and risk management needs;

c. a policy regarding the allowed usage of and reliance on End User Computing, in particular regarding the identification, registration and documentation of important end user computing solutions (e.g. when processing important data) and the expected security levels to prevent unauthorised modifications, both in the tool itself, as well as data stored in it;

d. documented exception handling processes to resolve identified ICT data integrity issues in line with their criticality and sensitivity.

[9] A data officer is responsible for data processing and usage.
[10] A data custodian is responsible for the safe custody, transport and storage of data.
[11] A data steward is responsible for the management and fitness of data elements – both the content and metadata.

58. For supervised institutions that fall under the scope of the BCBS 239 principles for effective risk data aggregation and risk reporting[12], competent authorities should review the institution's risk analysis of its risk reporting and data aggregation capabilities compared to the principles and the prepared documentation thereon, taking into consideration the implementation timeline and transitional arrangements in these principles.

(e) Controls for managing material ICT outsourcing risks

59. Competent authorities should assess whether the institution's outsourcing strategy, in line with the requirements of the CEBS outsourcing Guidelines (2006) and further to the requirement in paragraph 85 (d) of the EBA SREP Guidelines, adequately applies to ICT outsourcing, including intra-group outsourcing providing ICT services within the group. When assessing the ICT outsourcing risks, competent authorities should take into consideration that the ICT outsourcing risks can also be covered as part of the assessment of inherent operational risks under paragraph 240 (j) of the EBA SREP Guidelines, to avoid any duplication of work or double counting.

60. In particular competent authorities should assess whether the institution has an effective framework in place for identifying, understanding and measuring ICT outsourcing risk, and in particular, controls and a control environment in place for mitigating risks related to material outsourced ICT services that are commensurate with the size, activities and the ICT risk profile of the institution and include:

a. an assessment of the impact of the ICT outsourcing on the risk management of the institution related to the use of service providers (e.g. cloud service providers) and their services during the procurement process that is documented and is taken into account by senior management or the management body for the decision to outsource the services or not. The institution should review the ICT risk management policies and the ICT controls and control environment of the service provider to ensure that they meet the institution's internal risk management objectives and risk appetite. This review should be periodically updated during the contractual outsourcing period, taking into account the characteristics of the outsourced services ;

b. a monitoring of the ICT risks of the outsourced services during the contractual outsourcing period as part of the institution's risk management, that feeds into the institution's ICT risk management reporting (e.g. business continuity reporting, security reporting);

c. a monitoring and comparison of the received service levels with the contractually agreed upon service levels which should form part of the outsourcing contract or service level agreement (SLA); and

d. adequate staff, resources and competences to monitor and manage the ICT risks from the outsourced services.

[12] Basel Committee on Banking Supervision, Principles for effective risk data aggregation and risk reporting, January 2013, available online: http://www.bis.org/publ/bcbs239.pdf.

3.4 Summary of findings and scoring

61. Following the above assessment, competent authorities should form an opinion on the institution's ICT risk. This opinion should be reflected in a summary of findings which competent authorities should consider when assigning the score of operational risk in Table 6 of the EBA SREP Guidelines. Competent authorities should base their view on material ICT risks taking into account the following considerations to feed into the operational risk assessment:

a. Risk Considerations

i. The institution's ICT risk profile and exposures;
ii. The identified critical ICT systems and services; and
iii. The materiality of ICT risk regarding critical ICT systems.

b. Management and Controls considerations

i. Whether there is consistency between the institution's ICT risk management policy and strategy and its overall strategy and risk appetite;
ii. Whether the organisational framework for ICT risk management is robust with clear responsibilities and a clear separation of tasks between risk owners and management and control functions;
iii. Whether ICT risk measurement, monitoring and reporting systems are appropriate.; and
iv. Whether the control frameworks for material ICT risks are sound.

62. If competent authorities deem ICT risk to be material and the competent authority decides to assess and score this risk as a sub-category of operational risk the table below (Table 1) provides the ICT risk score considerations.

Table 1: Supervisory considerations for assigning an ICT risk score

Risk Score	Supervisory view	Considerations for inherent risk	Considerations for adequate management & controls
1	There is no discernible risk of significant prudential impact on the institution considering the level of inherent risk and the management and controls.	• The information sources to be considered under paragraph 37 did not reveal any significant ICT risk exposures. • The nature of the institution's ICT risk profile, in conjunction with the review of the critical ICT systems and the material ICT risks to the ICT Systems and Services, have not revealed any material ICT risks.	
2	There is a low risk of significant prudential impact on the	• The information sources to be considered under paragraph 37 did not reveal any significant ICT risk	

	institution considering the level of inherent risk and the management and controls.	exposures. • The nature of the institution's ICT risk profile, in conjunction with the review of the critical ICT systems and the material ICT risks to the ICT Systems and Services, revealed a limited ICT risk exposure (e.g. not more than 2 out of 5 of the predefined ICT risk categories).	• The institution's ICT risk policy and strategy is commensurate with its overall strategy and risk appetite. • The organisational framework for ICT risk is robust with clear responsibilities and a clear separation of tasks between risk owners and management and control functions. • ICT risk measurement, monitoring and reporting systems are appropriate. • The control framework for ICT risk is sound.
3	There is a medium risk of significant prudential impact on the institution considering the level of inherent risk and the management and controls.	• The information sources to be considered under paragraph 37 revealed indications of possible significant ICT risk exposures. • The nature of the institution's ICT risk profile, in conjunction with the review of the critical ICT systems and the material ICT risks to the ICT Systems and Services, revealed a heightened ICT risk exposure (e.g. 3 or more out of 5 of the predefined ICT risk categories).	
4	There is a high risk of significant prudential impact on the institution considering the level of inherent risk and the management and controls.	• The information sources to be considered under paragraph 37 provided multiple indications of significant ICT risk exposures. • The nature of the institution's ICT risk profile, in conjunction with the review of the critical ICT systems and the material ICT risks to the ICT Systems and Services, revealed a high ICT risk exposure (e.g. 4 or 5 out of 5 of the predefined ICT risk categories).	

Annex – ICT Risk Taxonomy

5 ICT risk categories with a non-exhaustive list of ICT risks with a potential high severity and/or operational, reputational or financial impact

ICT risk categories	ICT risks (non exhaustive[13])	Risk description	Examples
ICT availability and continuity risks	Inadequate capacity management	A lack of resources (e.g. hardware, software, staff, service providers) can result in an inability to scale the service to meet business needs, system interruptions, degradation of service and/or operational mistakes.	• A capacity shortfall may affect transmission rates and the availability of the network (internet) for services like internet banking. • A lack of staff (internal or third party) can result in system interruptions and/or operational mistakes.
	ICT system failures	A loss of availability due to hardware failures.	• Failure/malfunction of storage (hard disks), server or other ICT equipment caused by e.g. lack of maintenance.
		A loss of availability due to software failures and bugs.	• Infinite loop in application software prevents transaction execution. • Outages due the continued use of outdated ICT systems and solutions that no longer meet present availability and resilience requirements and/or are no longer supported by their vendors.
	Inadequate ICT continuity and disaster recovery planning	Failure of ICT planned availability and/or continuity solutions and/or disaster recovery (e.g. fall-back recovery datacentre) when activated in response to an incident.	• Configuration differences between the primary and secondary datacentre may result in the incapacity of the fall-back datacentre to provide the planned continuity of service.
	Disruptive and destructive cyber attacks	Attacks for different purposes (e.g. activism, blackmailing), which result in an overloading of systems and the network, preventing online computer services to be accessed by their legitimate users.	• Distributed Denial of Service attacks are performed by means of a multitude of computer systems on the internet controlled by a hacker, sending a large amount of apparently legitimate service requests to internet (e.g. e-banking) services.

[13] ICT risks are listed under the risk category they most impact but they may impact other risk categories

ICT risk categories	ICT risks (non exhaustive[13])	Risk description	Examples
ICT security risks	Cyber-attacks and other external ICT based attacks	Attacks performed from the internet or outside networks for different purposes (e.g. fraud, espionage, activism / sabotage, cyber terrorism) using a variety of techniques (e.g. social engineering, intrusion attempts through the exploitation of vulnerabilities, deployment of malicious software) resulting in taking control of internal ICT systems.	Different types of attacks: • APT (Advanced Persistent Threat) for taking control of internal systems or stealing information (e.g. identity theft related information, credit card information). • Malicious software (e.g. ransomware) that encrypts data with the aim of blackmail. • Infection of internal ICT systems with Trojan horses for committing malicious system actions in a hidden manner. • Exploitation of ICT system and/or (web) application vulnerabilities (e.g. SQL injection …) to gain access to the internal ICT system.
		Execution of fraudulent payment transactions by hackers through the breaking or circumvention of the security of e-banking and payment services and/or by attacking and exploiting security vulnerabilities in the internal payment systems of the institution.	• Attacks against e-banking or payment services, with objective to commit unauthorised transactions. • The creation and sending out of fraudulent payment transactions from within the internal payment systems of the institution (e.g. fraudulent SWIFT messages).
		Execution of fraudulent securities transactions by hackers through the breaking or circumvention of the security of the e-banking services that also provide access to the customer's securities accounts.	• Pump and dump attacks where the attackers gain access to e-banking securities accounts of customers and place fraudulent buying or selling orders to influence the market price and /or make gains based on previously established securities positions.
		Attacks on communication connections and conversations of all kinds or ICT systems with the objective of collecting information and/or committing frauds.	• Eavesdropping/intercepting unprotected transmission of authentication data in plain-text.
	Inadequate internal ICT	Gaining unauthorised access to critical ICT systems from within the institution for different purposes (e.g.	• Installing key stroke loggers (key loggers) to steal user IDs and passwords to gain unauthorised access

ICT risk categories	ICT risks (non exhaustive[13])	Risk description	Examples
	security	fraud, performing and hiding rogue trading activities, data theft, activism / sabotage) by a variety of techniques (e.g. abusing and/or escalating privileges, identity theft, social engineering, exploiting vulnerabilities in ICT systems, deployment of malicious software).	to confidential data and/or commit fraud. • Cracking/guessing weak passwords to gain illegitimate or elevated access rights. • System administrator uses operating systems or database utilities (for direct database modifications) to commit fraud.
		Unauthorised ICT manipulations due to inadequate ICT access management procedures and practices.	• Failure to disable or delete unnecessary accounts such as those of staff that changed functions and/or left the institution, including guests or suppliers who no longer need access, providing unauthorised access to ICT systems. • Granting excessive access rights and privileges, allowing unauthorised accesses and/or making it possible to hide rogue activities.
		Security threats due to lack of security awareness whereby employees do not understand, neglect or fail to adhere to ICT security policies and procedures.	• Employees that are deceived into providing assistance for an attack (i.e. social engineering). • Bad practices regarding credentials: sharing passwords, using 'easy' to guess passwords, using the same password for many different purposes, etc. • Storage of unencrypted confidential data on laptops and potable data storage solutions (e.g. USB keys) that can be lost or stolen.
		The unauthorised storage or transfer of confidential information outside the institution.	• Persons stealing or deliberately leaking or smuggling out confidential information to unauthorised persons or the public.
	Inadequate physical ICT security	Misuse or theft of ICT assets via physical access causing damage, loss of assets or data or to make other threats possible.	• Physically breaking into office buildings and/or data centres to steal ICT equipment (e.g. computers, laptops, storage solutions) and/or to copy data by physically accessing ICT systems.
		Deliberate or accidental damage to physical ICT assets	• Physical terrorism (i.e. terrorist bombs) or sabotage

ICT risk categories	ICT risks (non exhaustive[13])	Risk description	Examples
		caused by terrorism, accidents or unfortunate/erroneous manipulations by staff of the institution and/or third parties (suppliers, repairman).	of ICT assets. • Destruction of data centre caused by fire, water leakage or other factors.
		Insufficient physical protection against natural disasters resulting in partial or complete destruction of ICT systems/datacentres by natural disasters.	• Earthquakes, extreme heat, wind storms, heavy snowstorms, floods, fire, lightning.
ICT change risks	Inadequate controls over ICT system changes and ICT development	Incidents caused by undetected errors or vulnerabilities as a result of change (e.g. unforeseen effects of a change or a poorly managed change due to a lack of testing or improper change management practices) to e.g. software, ICT systems and data .	• Release into production of insufficiently tested software or configuration changes with unexpected adverse effects on data (e.g. corruption, deletion) and/or ICT system performance (e.g. breakdown, performance degradation). • Uncontrolled changes to ICT systems or data in the production environment. • Release into production of ill-secured ICT systems and internet applications, creating opportunities for hackers to attack the provided internet services and /or to breach the internal ICT systems. • Uncontrolled changes in the source code of internally developed software. • Insufficient testing due to the absence of adequate testing environments.
	Inadequate ICT architecture	A weak ICT architecture management when designing, building and maintaining ICT systems (e.g. software, hardware, data) can lead, over time, to complex, difficult, costly to manage and rigid ICT systems, that are no longer sufficiently aligned with business needs and are falling short compared to actual risk management requirements.	• Inadequately managed changes to ICT systems, software and/or data over a prolonged period of time, leading to complex, heterogeneous and difficult to manage ICT systems and architectures, causing many adverse business and risk management impacts (e.g. lacking flexibility and agility, ICT incidents and failures, high operating cost, weakened ICT security and resiliency, reduced data quality and reporting capabilities). • Excessive customisation and extension of

ICT risk categories	ICT risks (non exhaustive[13])	Risk description	Examples
			commercial software packages with internally developed software, leading to the incapacity to implement future releases and upgrades of the commercial software and the risk of no longer being supported by the vendor.
	Inadequate lifecycle and patch management	The failure to maintain an adequate inventory of all ICT assets in support of, and in combination with, sound life-cycle and patch management practices. This leads to insufficiently patched (and thus more vulnerable) and outdated ICT systems that may not support business and risk management needs.	• Unpatched and outdated ICT systems that may cause adverse business and risk management impacts (e.g. lacking flexibility and agility, ICT outages, weakened ICT security and resilience).
ICT data integrity risks	Dysfunctional ICT data processing or handling	Due to system, communication and/or application errors or failures, or erroneously executed data extraction, transfer and load (ETL) process, data could be corrupted or lost.	• IT system error in batch processing, causing incorrect balances in client's bank accounts. • Wrongly executed queries. • Data loss due to data replication (backup) error.
	Ill designed data validation controls in ICT systems	Errors relating to missing or ineffective automated data input and acceptance controls (e.g. for used third party data), data transfer, processing and output controls in the ICT systems (e.g. input validity controls, data reconciliations).	• Insufficient or invalid formatting/validation of data inputs in applications and/or user interfaces. • Absence of data reconciliation controls on produced outputs • Absence of controls on the executed data extraction processes (e.g. database queries) leading to erroneous data. • Use of faulty external data.
	Ill controlled data changes in the production ICT systems.	Data errors introduced due to lack of controls on the correctness and justified nature of data manipulations performed in the production of ICT systems	• Developers or database administrators directly accessing and changing the data in the production ICT systems in a non-controlled way e.g. in the case of an ICT incident.
	Ill designed and/or managed data architecture, data flows, data	Ill managed data architectures, data models, data flows or data dictionaries may result in multiple versions of the same data across the ICT systems, which are no longer consistent due to differently applied data	• The existence of different customer databases per product or business unit with different data definitions and fields, resulting in unreconciled and difficult to compare an integrate customer data at

ICT risk categories	ICT risks (non exhaustive[13])	Risk description	Examples
	models or data dictionaries	models or data definitions, and/or differences in the underlying data generation and change process.	the level of the whole financial institution or group.
ICT outsourcing risks	Inadequate resilience of third party or another Group entity services	The non-availability of critical outsourced ICT services, telecommunication services and utilities. Loss or corruption of critical/sensitive data entrusted to the service provider	• Unavailability of core services as a result of failures in suppliers (outsourced) ICT systems or applications. • Disruption of telecommunication links. • Power supply shortage.
	Inadequate outsourcing governance	Major service degradation or failures due to inefficient preparedness or control processes of the outsourced service provider. Ineffective outsourcing governance may result in a lack of appropriate skills and capabilities to fully identify, assess, mitigate and monitor the ICT risks and can limit institutions' operational capabilities.	• Poor incident handling procedures, contractual control mechanisms and guarantees built into the service provider agreement that increase key man dependency on third parties and vendors. • Inappropriate change management controls concerning the service provider ICT environment can cause major service degradation or failure.
	Inadequate security of third party or another Group entity	Hacking of the third party service providers' ICT systems, with a direct impact on the outsourced services or critical/confidential data stored at the service provider. Service provider staff gaining unauthorised access to critical/sensitive data stored at the service provider	• Hacking of service providers by criminals or terrorists, as an entry point into the institutions' ICT systems or to access /destroy critical or sensitive data stored at the service provider. • Malicious insiders at the side of the service provider try to steal and sell sensitive data.

5. Accompanying documents

5.1 Draft cost-benefit analysis / impact assessment

These Guidelines are designed to complement the EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP). As per Article 16(2) of the EBA regulation (Regulation (EU) No 1093/2010 of the European Parliament and of the Council), any Guidelines developed by the EBA shall be accompanied by an Impact Assessment (IA) annex which analyses 'the potential related costs and benefits'. Such annex shall provide the reader with an overview of the findings as regards the problem identification, the options identified to remove the problem and their potential impacts.

For the purposes of the IA section of the Consultation Paper, the EBA prepared a qualitative questionnaire to collect information on the baseline, i.e. the practices currently in place in Member States and, the expected costs and benefits in relation to ICT risk assessment and the provisions covered under these Guidelines. The questionnaire targeted national competent authorities. This annex presents the IA with cost-benefit analysis of the provisions included in the Guidelines described in this Consultation Paper. Given the nature of the study, the IA is high-level and qualitative in nature.

A. Problem identification

The EBA SREP Guidelines introduce assessment criteria for competent authorities when evaluating, amongst other elements, the institutions' business models, their internal governance and institution-wide controls and risks to capital. ICT risk is one important risk that competent authorities should consider in the implementation of these provisions, however, the EBA SREP Guidelines only elaborate to a limited extent on ICT risk under operational risk. Given the importance and the potential significant prudential impact of ICT risk on an institution and on the banking sector as whole, as mentioned in the 'Background and rationale' section of the current Guidelines, the lack of specific guidance and a more detailed assessment for supervisors to assess ICT risk in the EBA SREP Guidelines may lead to an incomplete risk assessment of an institution in the prudential supervisory framework.

The core gap that the current Guidelines aim to address is the lack of in depth guidance for the supervisory assessment of ICT risk in institutions and therefore room for lack of assessment of this risk, as well as inconsistency in assessing ICT risk across MS leading to a lack of comparability of supervisory practices across the EU which is crucial given the cross-border nature of ICT risk. Additionally the current level of detail in the EBA SREP Guidelines on how to assess ICT risk could lead to an insufficient measurement of ICT risks in the EU.

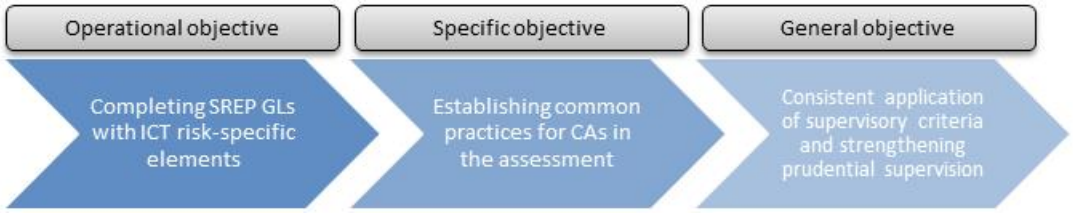
ICT is an intrinsic component of banks' operational functioning and with the elaboration in recent years of accessibility to banking products and communications through technology, ICT is fundamental to the implementation and development of an institution's business model. Concurrently the prudential risks that ICT may give rise to need to be managed by the institution. It is this risk and the related controls that these

Guidelines provide guidance on to supervisors in the context of the SREP, i.e. that there is an impact on the institution's business model, governance and capital deriving from ICT risk.

B. Policy objectives

The main objective of the Guidelines is to specify a set of principle-based rules that complement the EBA SREP Guidelines for competent authorities to apply, using the principle of proportionality, in their supervisory assessment of ICT risk. Precisely, the Guidelines aim to inform supervisors how they should supervise this risk and to create consistent practices and a common level-playing field across jurisdictions. In this way, the current Guidelines are expected to respond pro-actively to the challenges in the prudential supervision of ICT-related risks.

The diagram below summarises the objectives of the Guidelines:



C. Baseline scenario

Table 1 presents the baseline scenario by Member State on the 'compliance' of the institutions and the competent authorities with these Guidelines. Precisely, it presents in each Member State an overview of current implementation and practices in relation to the major sections of the Guidelines. This presentation gives an overview of potential further efforts that the competent authorities may make and an indication of corresponding costs and benefits of further compliance.

The information provided shows that all Member States have, for the assessment of ICT risk, mechanisms and measures in certain forms. However, there are also variations in the current level of practices across Member States in relation to future implementation of the Guidelines. Currently, while some Member States (e.g. CZ, FI, NL and PL) have practices in place that are fully or largely in line with the provisions of the Guidelines, the practices of some other Member States (BE, UK) do not show similarities with these provisions. On average, the current practices in Member States mostly cover the provisions of the Guidelines. Table 2 shows the share of implementation level indicated by the Member States in percentage. In terms of the sections of the Guidelines except two sections[14] of the Guidelines, all Member States either mostly or fully cover all the sections. In other words, the share of categories mostly implemented and fully implemented in total exceed 50% in all categories except in two sections.

[14] ICT strategy implementation (2.2.2) and controls for managing ICT data integrity risks (3.3. (d))

Table 1 - Current practices with respect to the content of the Guidelines, by Member State

	Title 2				Section 3.2			Section 3.3.								Annex
	2.2.1 ICT strategy development and adequacy	2.2.2 ICT strategy implementation	2.3 Overall Internal Governance	2.4 Risk management frameworks	3.2.1 Determination of the institution's ICT risk profile	3.2.2 Determination of the institution's critical ICT systems and services	3.2.3 Assessment of material ICT risks to ICT systems and services	ICT risk management policy processes and tolerance thresholds	Organisational management and oversight framework	Internal audit coverage and findings	(a) Controls for managing material ICT Availability and Continuity risks	(b) Controls for managing material ICT Security risks	(c) Controls for managing material ICT Change risks	(d) Controls for managing material ICT data integrity risks	(e) Controls for managing material ICT Outsourcing risks	ICT risk taxonomy
AT	1	1	3	3	1	1	1	1	1	1	1	1	1	1	1	:
BE	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2
CY	2	1	2	2	2	1	2	2	2	3	2	3	2	1	3	2
CZ	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
DE	1	1	2	2	2	2	2	2	2	2	2	2	2	1	2	1
DK	1	1	2	2	2	2	2	1	2	3	1	2	2	2	2	2
EE	2	2	3	2	2	2	3	:	3	2	2	2	1	1	2	:
EL	1	1	3	2	3	2	2	1	2	3	3	3	2	1	3	2
ES	2	1	2	2	2	2	2	2	2	3	3	2	3	2	2	2
FI	2	2	3	2	3	3	3	2	2	3	3	3	3	2	3	2
FR	2	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2
HR	2	1	3	1	1	2	1	2	2	2	1	1	1	1	1	1
IT	2	2	2	1	1	1	2	2	1	3	3	3	3	1	3	:

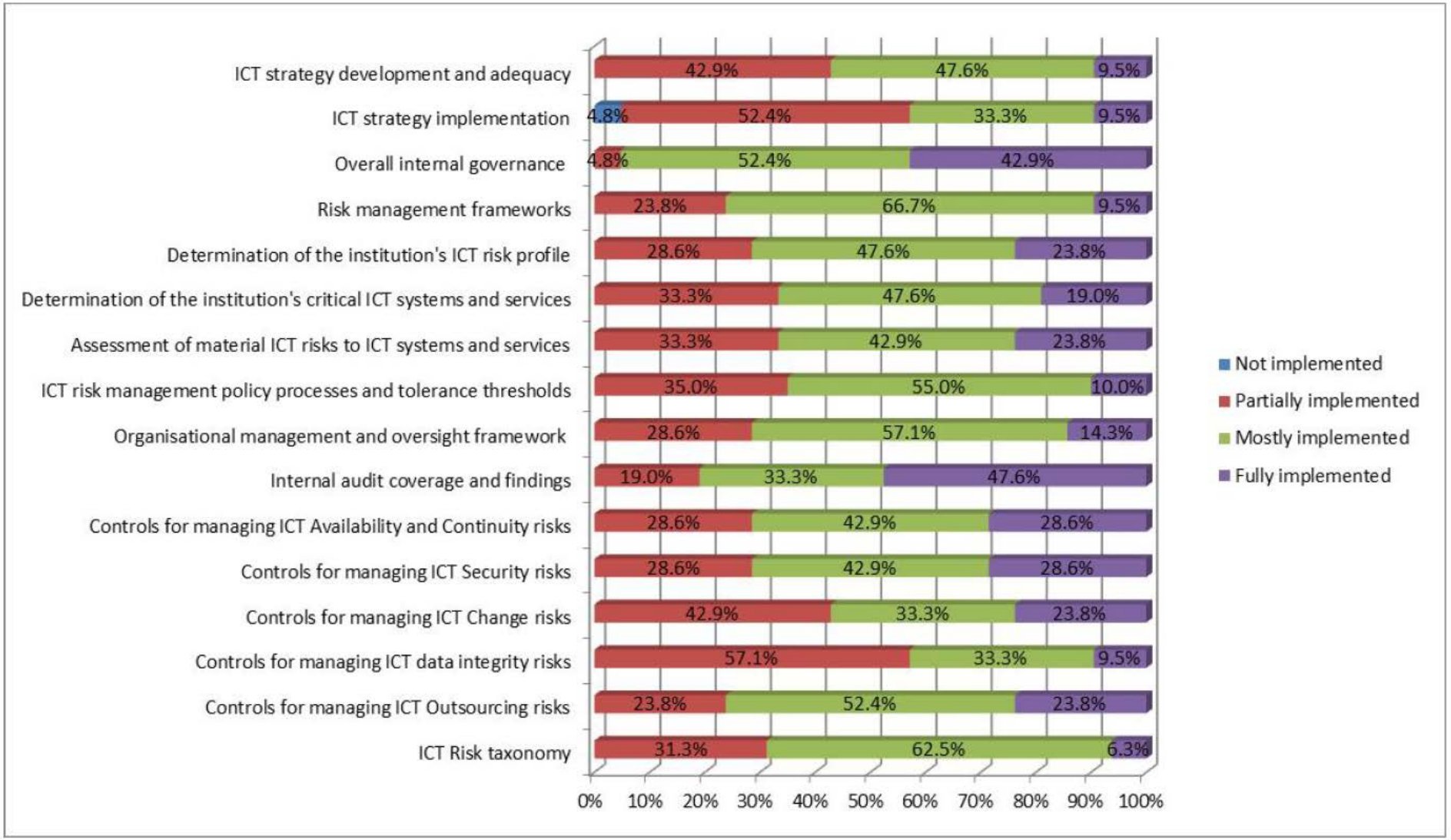
LU	1	1	2	2	3	1	1	1	1	3	2	2	1	1	2	1
NL	2	2	2	2	2	3	3	2	3	3	2	2	2	2	2	2
PL	3	3	3	2	3	3	3	3	2	3	3	3	3	3	2	:
PT	1	1	2	2	2	1	1	1	2	2	1	1	1	1	1	:
RO	1	2	2	1	1	2	2	2	1	1	2	2	1	2	2	1
SE	1	1	2	2	2	1	1	1	1	1	1	1	1	1	1	2
SK	2	1	2	1	1	2	1	2	2	2	2	1	1	2	2	1
UK**	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	:

* 0 (not implemented), 1 (partially implemented), 2 (mostly implemented), 3 (fully implemented).

**UK includes the average of the responses both from the Prudential Regulation Authority (PRA) of Bank of England and Financial Conduct Authority (FCA).

':' = not ranked

Table 2 - Current practices with respect to the content of the Guidelines



D. Assessment of the options considered and the preferred options

This section presents the major policy options considered in the drafting of the current Guidelines. In drafting the Guidelines many policy options were considered however here we assess four of these.

i. Development of ICT risk assessment Guidelines to complement the existing EBA SREP Guidelines or development of a separate methodology for assessment of ICT risk

As described above, ICT risk is an important operational risk which was so far addressed but to a limited extent in the EBA SREP Guidelines.

The assessment of ICT risk is undertaken with the intention of complementing the existing references in the operational risk assessment elaborated in the EBA SREP Guidelines. However it was noted that a complete ICT risk assessment would complement not only the operational risk assessment in section 6.4 of the EBA SREP Guidelines but also the business model assessment in Title 4 and the institution's internal governance and institution-wide controls assessment in Title 5 of the EBA SREP Guidelines. Furthermore, in order to complement the operational risk assessment, the methodology in the assessment of ICT risk broadly follows the same process.

To develop a separate methodology would create duplication of aspects already covered in the EBA SREP Guidelines and in parallel may potentially increase regulatory cost for the industry and competent authorities. For example there are a number of components in the ICT risk assessment Guidelines which are not only relevant in the context of operational risk but also in the elements mentioned in the paragraph above. To give context to the ICT risk assessment it is necessary to link them to the EBA SREP Guidelines' provisions and highlight that the ICT risk assessment Guidelines elaborate on the existing SREP provisions.

As such these Guidelines are designed to complement the existing EBA SREP Guidelines and do not introduce a new methodology.

ii. Inclusion or exclusion of a provision specific to ICT strategy to complement the business model assessment in the EBA SREP Guidelines

ICT strategy presents an important share of institutions' intangible assets, investments and operational costs and it forms a key part of business strategies, sources of competitive advantage as well as potential causes of material operational disruptions, investment write-offs or reputational damage.

As a result of this important link, the EBA considered including provisions specifically on the assessment of ICT strategy in the Guidelines. These provisions go beyond the general business model assessment (BMA) in the EBA SREP Guidelines and guide supervisors to incorporate the results of the ICT strategy assessment as a part of the BMA in the EBA SREP Guidelines.

If such provisions are not specified in these Guidelines then the BMA i) may not be able to identify whether the business model of an institution has *adequate ICT resources* to implement the

intended strategy and activities, and ii) may not be able to identify if the institution has *an adequate and sustainable business strategy* given the ICT resources available to it.

Therefore, a major disadvantage of excluding these specific provisions on ICT strategy may jeopardise both an adequate assessment of institutions' risk and viability in line with SREP Guidelines (in particular provisions 70b, 70c and 72e) and a full understanding of the institution's strategy. This may further have a prudential impact on institutions.

On the other hand, the inclusion of a provision on assessment of ICT strategy requires that when assessing ICT risk, competent authorities consider the alignment between the ICT strategy and the institution's business model. ICT risk is included under the BMA because of the strong links between the two: as highlighted in the EBA SREP Guidelines (70.b, 70.c and 72.e) ineffective ICT capabilities and strategies as well as insufficient execution capabilities have a strong impact in terms of sustainability of the institution. The outcome of the ICT strategy assessment should not be reflected in the scoring of ICT operational risk or that of internal governance and controls but, where relevant, should be considered as part of the BMA assessment, since the main effects it can have are reductions in earnings, rigidity in cost structures and loss of franchise in or disaffection with the institution by investors, or market participants.

Given these arguments, the EBA decided to include ICT strategy in these Guidelines in order to complement the assessment of business models in Title 3 of the SREP Guidelines.

iii. Specification or exclusion of material ICT risk controls

The section on 'Operational risk controls – 6.4.4' under 'risks to capital' in the EBA SREP Guidelines covers controls including organisation, management, audit and policies at a relatively high level. Due to the specificity of ICT risk and the fact that it is an area where guidance for general supervisors does not already exist, the EBA believes that there is scope to elaborate what type of controls could be used to mitigate the five broad ICT risk categories (from the risk taxonomy in the annex).

In the Guidelines (section 3.2.3) supervisors are asked to identify the material risks under the five broad risk categories listed in the taxonomy. To provide a consistent approach that is useful to the supervisors a specific list of controls applicable to these risk categories is included in the controls section 3.3. This specific list of controls is expected to facilitate the supervisors to understand exactly which mitigating factors can control the risks identified. This mapping therefore builds a bridge directly from the risks to the controls, going beyond general organisational and managerial aspects which are also included in these Guidelines and, is very specific to the risk categories identified. This is important for generalist supervisors who have not had experience to know what kind of controls are used in these circumstances.

A major downside of not including such guidance on risk controls is that the general controls and high level guidance only go so far in explaining how to mitigate ICT risks. ICT risks are particular in nature and their comprehensive assessment is new to the SREP assessment. The EBA therefore believes that these controls give the authorities the tools and knowledge to supervise and measure these risks. Consequently, the preferred option is to specify material ICT risk controls in the Guidelines.

iv. Inclusion or exclusion of a non-exhaustive risk taxonomy

ICT risks in banking come from a number of different sources and can have a significant prudential impact on institutions. Furthermore the in-depth supervision of ICT risks in banks is relatively new to many supervisors. For these reasons these Guidelines aim to bring about consistency in how supervisors assess the ICT risks to which an institution is exposed.

To bring about such a harmonised EU approach, a common understanding of ICT risk terminology was deemed necessary. As a result, it was considered necessary to identify the broad risk categories under which ICT risks fall and, for this reason, an ICT risk taxonomy was developed for supervisors to adhere to a uniform understanding of the main risk categories of ICT risk. The risk taxonomy contains non - exhaustive examples of ICT risks under the risk categories to facilitate this understanding. Up until now either competent authorities had their own national taxonomy or such a taxonomy did not exist.

This taxonomy aims to bring about a uniform understanding of five broad risk categories and facilitate a common language with a non-exhaustive list of risks under each category with descriptions and examples. The ICT risks under the five broad risk categories are not exhaustive allowing competent authorities the flexibility to consider other ICT risks in their assessment.

Additionally, the inclusion of this taxonomy also brings about a common assessment methodology of ICT risk as the Guidelines, specifically Title 3, use the five ICT risk categories in the identification of material ICT risks and in the elaboration of specific controls relevant for those risk categories. Without such a taxonomy the convergence in the assessment of ICT risks would be limited, as these risks are, by their nature, cross -border and there is a need to have a common understanding across MS.

The EBA therefore decided to include non-exhaustive risk taxonomy.

E. Cost-Benefit Analysis

The EBA prepared a qualitative questionnaire to investigate the overall expected costs and benefits of the Guidelines for the institutions and the competent authorities. Most of the responses to the questionnaire indicate that the costs associated with the implementation of the Guidelines will be higher for the competent authorities than the expected cost for the institutions. Most of the institutions already have in place similar internal measures and procedures for ICT assessment foreseen in the Guidelines. Potential sources of additional costs for institutions in the implementation of the Guidelines are (i) formalisation of their current measures and procedures because many banks do not have a formalised framework to develop the ICT strategy, (ii) further efforts to put the internal practices in line with the provisions of the Guidelines, as banks mostly have risk management and internal control functions in place but not all of them assess the ICT risks in relation to risk appetite or ICAAP, (iii) training and potentially additional IT staff to comply with the regulatory framework.

Some large Member States (ES, FR, NL and UK) expect large costs for the institutions while some other Member States (CY, CZ, PL and LU) indicate small costs.

Similarly, Member States expect costs associated with the implementation of the Guidelines for national competent authorities. The sources of these costs are (i) training of the current IT personnel and recruitment of additional IT experts, (ii) introduction of a new ICT supervisory framework or formalisation of such framework if already in place, (iii) preparation or update of manuals to assist and train the institutions for compliance, (iv) additional time and resources for on-site inspection. Most of the Member States (FI, FR, HR, NL and SE) indicate an expectation, on average, of medium to high levels of cost for the competent authorities.

The taxonomy is deemed to be a step forward in establishing a link between the concepts and concerns from the often very elaborate, detailed and highly technical existing IT audit frameworks (Cobit, CMMI, ISO etc.) that are little known and understood by non-IT experts and the practical and more intuitive language and thinking frameworks of generalist supervisors regarding the main ICT risks. It is a costly activity but is also crucial to build a sound framework for ICT assessment.

On the benefits side, overall the Member States expect the benefits to exceed the costs. Most of the Member States that indicate low benefits from the implementation of the Guidelines are also the ones that remain at the highest level in the baseline (CZ, PL), i.e. the Member States in which the current practices are already highly in line with the provision of the Guidelines.

ICT is a crucial element of modern banking services with a significant impact on the institution's competitiveness and cost effectiveness. The Guidelines help draw a sound framework for better management of ICT risk and other ICT practices within the institutions. The Guidelines will also help establish the necessary management focus and support for important risks such as the ever-growing cyber risks and important evolutions like FinTech that may have a pervasive impact on the institution's business model, competitiveness and profitability. At more micro-level the implementation of the Guidelines is expected to (i) increase ICT risk awareness for both institutions and competent authorities, (ii) increase data quality and integrity, (iii) improve the monitoring of critical systems, (iv) standardise ICT risk categories and (v) standardise risk taxonomy which implies homogenous language and common understanding.

Across all Member States, when average costs and the average benefits are compared, a majority of the participants (about 65%) believe that the expected net benefits are positive, i.e. expected benefits exceed the expected costs. Six Member States (FI, FR, HR, NL, PL and UK) state that the expected average net benefits are negative. For these Member States, although the potential costs for the institutions are somewhat smaller, the expected costs that may fall on the competent authorities are large and are deemed by them to exceed the benefits of the Guidelines.

5.2 Feedback on the public consultation

The EBA publicly consulted on the draft proposal contained in this paper.

The consultation period lasted for 3 months from 06 October 2016 to 06 January 2017. A total of 16 responses were received, 12 of which were published on the EBA website. The Banking Stakeholders Group did not provide any opinion.

This section presents a summary of the key points and other comments arising from the consultation, the analysis and discussion triggered by these comments and the actions taken to address them if deemed necessary.

In many cases several industry bodies made similar comments. In such cases, the comments, and EBA's analysis are included in the section of this paper where EBA considers them most appropriate.

Changes to the Guidelines have been incorporated as a result of the responses received during the public consultation.

Summary of key issues and the EBA's response

All comments were unanimously supportive and positive on the need to define a common framework for the assessment of Information and Communication Technology risk under the Supervisory Review and Evaluation process (SREP) highlighting the importance of technology in banking as well as the significance of ICT risk and its continuous evolution along with the increased regulatory focus on this area.

All respondents welcomed the effort to promote common procedures and methodologies in assessing ICT risk and recognised it will enhance consistency in practices and a level-playing field across jurisdictions. The industry found these Guidelines consistent with the EBA SREP Guidelines and generally viewed ICT risk as part of operational risk which should be managed and controlled as part of an integrated risk framework.

These Guidelines were also welcomed as a positive step in addressing the need for a tailored regime for non-bank and non-systemic investment firms taking into account the distinct characteristics of such firms. The industry has also highlighted and appreciated the fact that these Guidelines do not introduce additional reporting obligations to institutions.

The main points raised by the industry with regard to the draft Guidelines were the following:

1) The need to ensure consistency with other relevant regulations and initiatives across jurisdictions at a global level was highlighted along with the industry's availability and readiness to further discuss how it can support the EBA in fostering the development of a globally harmonised approach to technology risk in banking.

2) The ICT risk taxonomy included in the Annex of these Guidelines raised a number of comments due to identified overlaps in the mapping and an unclear distinction between causes, events and impacts. In general, a common issue was that an event could lead into more than one ICT risks and thus may not facilitate the ICT risk assessment. To this end, additional clarity was required for correctly mapping events to ICT risk categories.

3) A common question was whether institutions should align their existing own risk taxonomies with the proposed ICT risk taxonomy included in the Annex or if these should be maintained.

4) The importance of the proportionality principle in the application of these Guidelines was highlighted by the majority of respondents. In some cases, additional clarity was requested on its application across jurisdictions and global institutions.

5) The level of involvement and the required role of the management body as well as the possibility of delegation raised concern among a number of respondents.

6) Further guidance was requested in relation to the assessment of institutions' risk reporting and data aggregation capabilities compared to the BCBS 239 principles for effective risk data aggregation and risk reporting.

7) Differentiation between external and intra-group ICT outsourcing risk was requested by some respondents given the different risks may arise from each outsourcing risk type.

The EBA carefully examined all the comments received (see table below) and amended the text of the Guidelines accordingly.

Summary of responses to the consultation and the EBA's analysis

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
General comments			
Principle of proportionality	Whereas respondents in general welcomed the inclusion of the proportionality principle as guiding principle for the Guidelines, several respondents expressed concern about how this will be applied by competent authorities, especially in the case of global banks and across jurisdictions. Further dialogue was also welcomed between the EBA, the competent authorities and the industry to discuss the application of the proportionality principle. The importance of proportionality principle was highlighted by a number of respondents who specifically suggested it should be followed in all the stages of the assessment and adequately taken into account when determining the scale and detail of the ICT risk assessment. In the same context, a respondent commented that the Guidelines seem to be more focused on large institutions without adequately considering the nature of smaller institutions.	The EBA notes that the overall principle of proportionality applies throughout the Guidelines and competent authorities should apply these Guidelines proportionately with respect to the categorisation of institutions as defined in the EBA SREP Guidelines. The categorisation of institutions, as provided in the EBA SREP Guidelines, will drive the level of proportionality and minimum supervisory engagement, in particular the frequency, scope and intensity of the supervisory review of an institution, and also the supervisory expectations of the standards the institution is expected to meet. Furthermore, the depth and detail of the ICT risk assessment should be proportionate to the size, structure and operational environment of the institution as well as the nature, scale and complexity of the institution's activities.	No changes made.
Level of application	A respondent noted that while these Guidelines are addressed to the competent authorities, paragraph 1 states that institutions must make every effort to comply with these Guidelines. Therefore, further clarification was suggested as regards the applicability of these Guidelines. In the same context, a respondent requested further details on the criteria around ICT risk assessment such as the level of independence required and whether the second or third line of defence could perform such an assessment. It was further proposed to introduce a	In view of the Guidelines being designed to supplement the EBA SREP Guidelines, the EBA would like to clarify that the assessment to these Guidelines should be performed by the competent authorities in the light of their continuous SREP exercise. The EBA notes that the competent authorities should state their intention regarding compliance with the Guidelines and then implement them in their practices. The EBA will be assessing the	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	prescribed assessment questionnaire to allow institutions respond effectively on their compliance status for these Guidelines.	implementation of the Guidelines, including any deviations from them, as part of its ongoing work on assessing convergence of supervisory practices.	
	Some respondents requested further details on the implementation period and frequency of these Guidelines. In particular, an implementation period of at least 12 months was suggested by one respondent.	In line with the implementation of Guidelines produced by the EBA, the date of application is usually 6 months after the date of publication. In line with the SREP Guidelines, the frequency, intensity and granularity of the assessments, and the level of engagement, depends on the categorisation of the institution.	The implementation date for these Guidelines has been set as 1 January 2018.
Consistency with other regulations and initiatives	Several respondents raised concerns about a danger of overlapping and inconsistent requirements being placed upon institutions in scope of the Guidelines due to a number of regulations and initiatives currently in place or being developed which address similar issues of ICT risk, and suggested a call for harmonisation of approaches across jurisdictions. Several respondents suggested the EBA's leadership in this regard, especially around topics like cyber which is often a cross-jurisdictional problem.	The EBA agrees with the concern regarding numerous initiatives currently in place or being developed in relation to ICT risk. In the spirit of limiting any inconsistencies with widely known and used definitions and terminologies as well as facilitating a common understanding on the ICT risk topic, the EBA will take into account these suggestions and possibly reconsider the definition for the ICT risk in the context of the forthcoming updates to the EBA SREP Guidelines. The EBA is striving to ensure coordination and cooperation with other authorities to avoid inconsistent requirements in its products, and aims to harmonise the requirements within the European Union.	No changes made.
Principle of flexibility	A number of respondents noted the importance of maintaining the principle of flexibility in relation to the ICT risk management as such risks are not clear-cut in nature.	The EBA acknowledges the importance of flexibility and notes that these Guidelines offer sufficient flexibility by means of allowing competent authorities to consider other ICT risks in their assessment as well as using the principle of	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		proportionality in their supervisory assessment.	
Incorporation to operational risk assessment	Some respondents requested further clarifications on how the ICT risk assessment will be factored into the evaluation of operational risk for ICAAP purposes and specifically, whether banks need to have a specific assessment on ICT risk or adjust their existing IT risk assessment processes to align with these Guidelines. It was further questioned whether this will contribute to the expert judgement to be used by the competent authorities for assessing institutions' operational risk exposure. A respondent noted that the current calculation of operational risk already includes ICT risk therefore by calculating one component of operational risk should not add any capital requirement, but actually reduce it, when measures are taken to increase the controlling of that risk. A respondent requested further clarity on how the supervisory assessment on ICT risk is expected to translate to capital requirements for operational risk and whether competent authorities are expected to assess ICT risk from a macro-economic stress test perspective (i.e. P2G). A respondent noted that a coherent approach to operational and ICT risk is required. Another respondent noted that institutions' new product approval policy already defines how risk and change of products are managed and questioned on how these Guidelines will be applied by competent authorities in their operational risk assessment.	These Guidelines aim to further specify the assessment of ICT risk as a component of operational risk under Article 85 of Directive 2013/36/EU. This assessment will result in a summary of findings which, based on a set of considerations, will inform the operational risk score of the EBA SREP Guidelines – part of the assessment of 'Risks to capital' – which will inform among others the determination of additional own funds requirements. As noted in paragraph 16, ICT risk may be assessed and scored individually as a sub-category of operational risk if deemed material by the competent authorities. In such a case, the scoring table (Table 1) in these Guidelines should be used to reach a score. Therefore, the application of the EBA SREP Guidelines in conjunction with these Guidelines should not result in double counting of capital requirements. It is important to note that these Guidelines do not intend to create duplication of aspects already covered in the EBA SREP Guidelines (and in parallel potentially increase regulatory cost for the industry and competent authorities). The assessment of ICT risk is undertaken with the intention of complementing the existing references in the operational risk assessment elaborated in the EBA SREP Guidelines and therefore, the methodology in the assessment of ICT risk broadly follows the same process. Competent authorities should use expert judgement to assess whether an institution has	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		potential exposure to ICT risk drivers (once these have been identified).	
Industry-wide suppliers	A respondent suggested that a better coordinated approach to industry-wide suppliers (e.g. national telecoms providers, ATM and payment transmission networks) might reduce the expected burden on regulatory bodies and firms rather than having multiple points of view of the same supplier. Such an approach might include supplier resilience, security, governance, and risk management. This will facilitate the assessment of concentration risk to the aforementioned industry-wide suppliers.	The EBA welcomes and appreciates this suggestion but would like to clarify that this topic is outside the scope and mandate of these Guidelines.	No changes made.
Additional areas	Some respondents suggested that external system risk IT components should be also addressed in these Guidelines.	The EBA welcomes this suggestion and wishes to note that these Guidelines offer sufficient flexibility to the competent authorities on the application of the ICT risk assessment. Moreover, the ICT risks under the five broad risk categories are not exhaustive allowing competent authorities the flexibility to consider other ICT risks in their assessment.	No changes made.
	One respondent proposed to include specific actions that will serve to cover strategic risks in the introduction to the document since the focus of the Guidelines seems to be on ICT operational risks.	The Guidelines focus mainly on the ICT risk assessment in the context of operational risk assessment under SREP. Nevertheless, from a strategic risk perspective, they contribute to the assessment of internal governance and institution-wide controls under Title 5 of the EBA SREP Guidelines, through the assessment of the institutions' governance and strategy on ICT (Title 2), as well as potentially informing the assessment of the business model assessment under Title 4 of the EBA SREP Guidelines.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
Specific questions in relation to the Consultation Paper EBA/CP/2016/14			
2. Subject matter, scope and definitions			
Subject matter	A respondent questioned whether the information required in these Guidelines need to be available only at individual level or at group level. It was suggested to be available only at individual level because of the significant amount of necessary documentation.	Competent authorities should apply these Guidelines in accordance with the level of application determined in Article 110 of Directive 2013/36/EU following the requirements and waivers used pursuant to Articles 108 and 109 of Directive 2013/36/EU.	No changes made.
Definitions	Several respondents observed that greater accuracy would be desirable in the definitions so as to avoid inconsistencies within the Guidelines and with respect to other European standards (such as the NIS Directive). Furthermore, several respondents suggested to use ISO definitions or similar for the definitions in paragraph 9. One respondent indicated that change risk and outsourcing risk are causes of three risk principle risks (confidentiality, integrity or availability) rather than separate, quantifiable risks in their own right. A respondent proposed to include reference to a common taxonomy that takes into consideration best practices and appropriately includes definitions for ICT security risk and cyber risk, leaving at the same time flexibility in implementation.	These Guidelines are addressed to all supervisors, including general supervisors in the framework of the overall SREP assessment. Therefore the language used is meant to be accessible and understandable for non-IT specialists. In this respect, the Guidelines aim to bridge the gap between the technical IT frameworks used by IT experts, and the translation needed to guide generalist supervisors. In the spirit of limiting any inconsistencies with widely known and used definitions and terminologies as well as facilitating a common understanding on the ICT risk topic, the EBA will take into account these suggestions and possibly reconsider the definition for the ICT risk in the context of the forthcoming updates to the EBA SREP Guidelines. As mentioned above, these Guidelines are addressed to competent authorities and aim to address the lack of in depth guidance for the supervisory assessment of ICT risk in institutions.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
ICT and ICT risk definitions	One respondent suggested that ICT should be defined in the Guidelines even if this is already the case in the SREP Guidelines and that the ICT definition of the SREP Guidelines would benefit from being refined and updated. A few respondents suggested that information and communication technology (ICT) should refer to all the technology of telecommunications, hardware, software and other related which enable users to access, store, transmit and manipulate information. Some respondents proposed further clarifications on the ICT risk definition which could also capture confidentiality risk and provide a more comprehensive and holistic view.	As mentioned above, the EBA will take into account these suggestions and possibly reconsider the definition for the ICT risk in the context of the forthcoming updates to the EBA SREP Guidelines. The notion of confidentiality risk is already included in the definition of ICT data integrity risk.	No changes made.
ICT services definition	Further clarifications were requested in relation to the ICT services; in particular what processes should be considered as important at international level and possibility of including reference to "business-processes with ICT-relevance" as most of the ICT systems are used for business processes. Some other respondents suggested ICT services to refer to the application of business and technical expertise to enable organisations in the creation, management and optimisation of or access to information and business processes. It was also noted that the ICT services market can be segmented by the type of skills that are employed to deliver the service (design, build, run). Gartner IT Glossary was referred to for the aforementioned definitions.	The EBA wishes to clarify that the existing ICT services definition is indeed wider and comprehensive aiming to cover all applicable processes.	No changes made.
ICT availability and continuity risk	Some respondents suggested that ICT availability risk should refer to the situation that availability of ICT systems and data are adversely impacted in their ability to perform their agreed function when required. This	The EBA welcomes this suggestion and notes that the existing definition of ICT availability and continuity risk is considered to be sufficiently holistic and comprehensive capturing the	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	includes the inability to recover the IT services for service recipients in a timely manner. Availability is determined by reliability, maintainability, serviceability, performance and security. In addition, ICT continuity (information technology continuity) should be determined by a holistic approach to managing technology systems in the event of a major disruption. ITIL V3 was referred to for the aforementioned definitions.	aforementioned suggestions.	
ICT security risk	A respondent suggested that ICT security risk should also encompass the risk from unlawful or unsolicited access to ICT system such as denial of services. Some other respondents proposed that ICT security risk should refer to the risk that availability of ICT systems, confidentiality, and integrity of data are adversely impacted by unauthorised user access. ICT security refers to the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security.	The EBA welcomes all the suggestions and agrees that the ICT security risk definition should be clarified to explicitly mention both ICT systems and data. In addition, the EBA wishes to clarify that the ICT security risk definition is deemed to cover both intentional and unintentional unauthorised access to ICT systems.	The ICT security risk definition in paragraph 8 has been amended to include "data" in the definition of ICT security risk.
ICT change risk	A respondent proposed to limit the definition of ICT change risk to failure in the project management process as the initial definition is broad and subjective (e.g. failure in implementing change may be caused by unavailability or integrity or security risks on ICT assets, reference to timely manner may be considered arguable).	The EBA welcomes the comment and notes that the existing definition of ICT change risk is considered as sufficiently comprehensive. Any explicit restrictions on its definition might limit the perimeter of the risk and adversely affect the scope of the ICT risk.	No changes made.
ICT data and assets definition	One respondent suggested that ICT data should be defined and proposed the definition of "data stored or processed by ICT system." Furthermore the respondent	The EBA understands the need for adding further definitions in the spirit of becoming more prescriptive, nevertheless the existing level of	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	indicated that ICT assets should also be defined.	detail is deemed sufficient for the competent authorities to address the risks arising to market integrity and the financial viability of institutions from ICT.	
ICT outsourcing risk	A respondent argued that outsourcing risk is not limited to ICT as it also captures business processes and should be defined as the risk linked to the choice of the service provider and its potential default. A few respondents suggested renaming the category "ICT outsourcing risk" to "ICT supplier risk" to provide a broader coverage than only outsourcing. Several respondents asked to differentiate in the Guidelines between intra-group outsourcing and outsourcing to third parties, since the risk arising from both types of outsourcing might be different and control mechanisms can be enforced in different ways. The respondents suggested adding in the Guidelines that there is a difference in terms of risk between outsourcing with third parties and intra-group outsourcing.	The EBA agrees that outsourcing can involve transaction processing and business processes and notes that outsourcing activities can introduce a number of risks (e.g. reputation risk, operational risk etc.). These Guidelines aim to capture the operational risk arising from outsourcing activities related to ICT. In line with the CEBS Outsourcing Guidelines, the definition of ICT outsourcing risk captures the risk arising from engaging with an outsourcing service provider i.e. can be external or internal to the group. It is important to note that ICT outsourcing risk definition captures both dimensions as these Guidelines do not differentiate external and intra-group ICT outsourcing for the purposes of assessing ICT outsourcing risk.	No changes made.
Title 2 - Assessment of institutions' governance and strategy on ICT			
2.1 General principles **ICT internal governance**	A respondent suggested adding reference to the three lines of defence model so as to ensure a more uniform interpretation of the spirit of the rules across the banking industry. Some other respondents also suggested adding regulatory expectations on the second line of defence so as to emphasise the robust management oversight.	The assessment of the overall internal governance referred to in these Guidelines to be conducted by the competent authorities will refer to the EBA Guidelines on internal governance, which completes the various governance provisions in Directive 2013/36/EU and specifies requirements for the three lines of defence. It is noted that the "three lines of defence" model - being the business line, the independent risk management and compliance functions and lastly the independent	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		internal audit function – has been used in the EBA Guidelines on internal governance for identifying the functions within institutions responsible to address and manage the risks.	
	A respondent highlighted the importance of a strong relationship between ICT and the business units as such a partnership will promote maximum effectiveness of the ICT function.	The EBA welcomes this comment and notes that the importance of a strong link between ICT and the business is deduced through the requirement of assessing the alignment between the ICT strategy and the institution's business model.	No changes made.
2.1 General principles **Involvement of management body**	Some respondents proposed that the Guidelines should explicitly acknowledge that the management body can internally delegate the execution of the principles, functions and expertise relating to ICT risk with the management body retaining the top management and supervisory function.	In the context of organisational management and oversight framework assessment, paragraph 49 gives the possibility to the management body to delegate some aspects of the independent control functions' findings to a committee. Nevertheless, it is important to note that delegation does not in any way release the management body in its supervisory function from collectively fulfilling its duties and responsibilities. It is possible for delegates to support the supervisory function in the ICT area and facilitate the development and implementation of a sound internal governance framework however it should be highlighted that management body's responsibilities cannot be delegated.	No changes made.
2.2 ICT strategy	Some respondents disagreed including the need of "keeping ICT up-to-date" and the treatment of important and complex ICT changes in this section and proposed to cover it in other sections as the ICT strategy should set a framework for long-term management of the ICT estate	An updated ICT and adequate planning or implementation of important and complex ICT changes within the ICT strategy is deemed important given the strong links between the ICT strategy and the business strategy (i.e. ineffective ICT capabilities and strategies as well as insufficient	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	and approach to change.	execution capabilities have a strong impact in terms of sustainability of the institution).	
	A respondent suggested removing bullet point 25c on the "engagement of the independent control and audit functions to provide assurance that the risks associated with ICT strategy implementation have been identified, assessed and effectively mitigated and that the governance framework in place to implement the ICT strategy is effective" as it cannot be expected that the internal audit or independent control is performed prior to any strategy implementation.	The engagement of the independent control and internal audit functions does not refer to internal audit assessing the ICT strategy as such but in providing assurance on the risks associated with the ICT strategy implementation. In line with the EBA Guidelines on internal governance, the internal audit function should assess the appropriateness of the institution's governance framework. Furthermore, while the business line – as the first "line of defence" – takes and manages the risks that it incurs in conducting its activities, the internal audit function is in charge of the independent review of the first as well as the second "line of defence".	No changes made.
	A respondent questioned whether "senior business management" and "management body" refer to in points 24a and 24d respectively relate to the same function. Further clarity was requested on how competent authorities will assess the adequacy of senior business management's involvement as senior business management is rarely involved in the operational work of implementing and follow-up.	The EBA wishes to clarify that paragraphs 26a and 26d refer to different functions as the first one refers to the senior management which is responsible for the day-to-day management of the institution (in line with Article 3(9) of the Directive 2013/36/EU) and the second one to the management body which is responsible, among others, to set, approve and oversee the implementation of the overall business strategy. It should be noted that senior management is accountable to the management body.	Paragraph 26a has been amended to refer only to "senior management" as defined in the Directive 2013/36/EU.
	On the same note, the approval of implementation plans and the monitoring of the ICT strategy by the institution's management body were questioned by some respondents	As highlighted in the EBA SREP Guidelines there are strong links between the ICT risk and the business model analysis and as a result, competent	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	who suggested that the management body should decide on the ICT strategy and follow major change initiatives on an aggregated level but delegate implementation and monitoring to appropriate functions. Another respondent suggested that ICT strategy should be part of an institution's business strategy.	authorities should consider the alignment between the ICT strategy and the institution's business model. To this end, the senior management of the business line is expected to be involved in the definition of the institution's strategic ICT priorities to facilitate the alignment between ICT strategy and business model. Once the ICT strategy is properly developed and formulated, it needs to be approved by the institution's management body in the context of its supervisory function as the management body has the ultimate and overall responsibility for the institution.	No changes made.
	Some respondents noted that it is not clear how competent authorities will assess the adequacy and also measure implementation plans for ICT strategy purposes.	The provisions of section 2.2.1 on ICT strategy development and adequacy should be used as guidance by competent authorities to support supervisory judgement. These Guidelines set the framework for ICT risk assessment having in mind the need to preserve a certain level of supervisory judgement.	No changes made.
	It was further suggested that in the case of significant ICT outsourcing, ICT strategy should always include options for action and exit processes in the event of unintended or unexpected termination of outsourcing. However, this should not be considered as mandatory in the case of intra-group outsourcing given the different nature of relation between the institution and the service provider.	The specific requirements for external and intra-group outsourcing are described in the CEBS Guidelines on outsourcing, including requirements for contingency plans and exit strategies. The CEBS Guidelines prescribe that the management of non-material and intra-group outsourcing should be proportionate to the risks presented by these arrangements.	No changes made.
	Another respondent noted that if competent authorities need to take into consideration the ICT cost cutting measures an institutions is implementing (point 37f), it	The reference to the implementation of aggressive ICT cost cutting measures by the institution could be seen by the competent authorities as an indication of potential increased exposures to all	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	will indicate that competent authorities should form an opinion on the institutions' investment plans. This may endanger competent authorities' supervisory role.	the ICT risk categories. This should be interpreted in the context of reviewing the institution's ICT risk profile rather than forming an opinion on the institution's investment plans. The EBA does not consider the assessment of ICT investment plans of institutions to be intrusive as long as its focus is to assess the potential impacts of investment plans on the risk management of the institution.	
2.2.1 ICT strategy development and adequacy	Some respondents suggested that paragraph 24 - on the development and adequacy of ICT strategy - could also include a strategic approach to suppliers.	The EBA agrees with the recommendation and notes that such requirements would be implicitly expected in the ICT strategy. However, the purpose of these Guidelines is not to provide the detailed information should be expected during the ICT risk assessment but to further specify the common procedures to be followed for the SREP in relation to ICT risks.	No changes made.
2.3 Overall internal governance	Some respondents proposed to include a materiality element in paragraph 26b and rephrase the sentence to "that the management body should know and address the *material* risks associated with the ICT rather than all the risks associated with the ICT."	In line with the EBA Guidelines on Internal Governance, the management body should be provided with relevant information about the identification, measurement or assessment and monitoring of risks. This reporting framework should be well defined, documented and duly approved by the management body.	No changes made.
Title 3 - Assessment of institutions' ICT risks exposures and controls			
3.1 General considerations	Additional information was requested regarding EBA's expectations on the consistency between IT risk assessment process and the broader operational risk management framework (e.g. uniform assessment methodology or consistency at more detailed level). In addition, further clarity was requested in relation to (i)	As mentioned above, these Guidelines are addressed to the competent authorities and the ICT risk assessment is undertaken with the intention of complementing the operational risk assessment. Therefore, these Guidelines are designed to complement the existing EBA SREP	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	the metrics, criteria and level of detail to be used to assess sources of information gathered by competent authorities referred to in paragraph 35, (ii) weighting of each component and (iii) any aggregation techniques that lead to the final score.	Guidelines and do not introduce a new methodology. Similar to the EBA SREP Guidelines, these Guidelines should be seen as guidance and not as restriction or limitation to supervisory judgment. This guidance does not mean scoring is automatic as the scores are assigned on the basis of supervisory judgment. Competent authorities should use the accompanying 'considerations' provided for guidance to support supervisory judgment. Competent authorities are not prohibited from applying more granular scoring on top of the base requirements specified in the Guidelines if they believe it is useful for supervisory planning.	
	Some respondents questioned the reference to "peer benchmarking" (through the reference to paragraph 127 of EBA SREP Guidelines) and argued that "peer benchmarking" may not be a meaningful approach for the purposes of operational risk assessment as operational risk varies between institutions.	In relation to the "peer benchmarking", paragraph 127 of Title 6 of the EBA SREP Guidelines refers to the comparison with peers for identifying potential exposure to risks to capital rather than for amending assessment scores. In the same paragraph, it is also noted that for such a comparison peers should be defined on a risk-by-risk basis. The EBA recognises the differentiations between institutions in terms of operational risk assessment and notes that competent authorities will use supervisory judgement during such an assessment which is intended to be institution-specific.	No changes made.
	A respondent suggested that a mix of controls described in Title 3 could be sufficient for mitigating ICT risks rather	The EBA wishes to highlight the importance of developing and maintaining a strong and	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	than assessing on a standalone basis.	comprehensive internal control framework and a strong control culture that encourages a positive attitude towards control within the institution. Competent authorities should assess the specific controls in place by institutions to address material ICT risks. The non-exhaustive list of controls provided in Title 3 should be used as guidance for competent authorities during institutions' internal control framework assessment around ICT risks.	
	It was also highlighted that ICT risks information is extremely sensitive and/or confidential and the development of information gathering processes for benchmarking and analytical assessment purposes would be a complex task. A respondent noted that production of ad-hoc information is always costly for institutions and requested whether it is possible to include detailed definitions of information requirements by providing institutions with templates and predefined submission dates. It was further suggested that ad-hoc reporting should be limited to urgent or unforeseeable instances giving institutions sufficient time for preparation e.g. 3 months.	The EBA understands the institutions' concerns around the introduction of additional reporting requirements and wishes to clarify that these Guidelines do not introduce additional reporting obligations as they assume that the assessments specified are made on the basis of information already being collected or readily available information at the institution to which the competent authority has an easy and sufficient access, and/or already collected information. However, where necessary, competent authorities should be able to request additional information from the institution.	No changes made.
3.2 Identification of	Several respondents suggested adding more clarity in the Guidelines on the concept of material ICT risk for example	Material ICT risks to which the institution is or might be exposed should be identified following a	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
material ICT risks	by including reference quantitative parameters (e.g. percentage of total assets) for the concept of materiality of the ICT risk.	review of the institution's ICT risk profile and critical ICT systems and services as described in Title 3.2. In general, the concept of materiality should be seen within the context of the EBA SREP Guidelines where risks to capital are described as risks which should they materialise, will have a significant prudential impact on the institution's own funds over the next 12 months.	
3.2.1 Review of the institution's ICT risk profile	A respondent proposed a stronger orientation of the referenced risks to the criticality of the respective business processes and underlying IT systems.	Critical business processes and their underlying IT systems should indeed be taken into account during the review of the institution's ICT risk profile. In addition, for the purposes of assessing ICT availability and continuity risk framework, competent authorities should identify the critical ICT processes and the relevant supporting ICT systems by analysing the dependencies between the critical business processes and supporting systems.	No changes made.
	The following were suggested to be added to the institution's ICT risk profile review list presented in paragraph 37: • Crisis management - to align with the relevant references in Title 3.3.4 on ICT control framework. • Potential impact on customers in a similar manner to the consideration of the risk to domestic and international financial systems. This could serve in distinguishing institutions with retail customers and investment firms with no retail customers which do not hold client assets.	The EBA welcomes the comments and agrees with the reference to crisis management in reviewing the institution's ICT risk profile, nevertheless the list of information presented in section 3.2.1 should not be considered exhaustive as it gives the competent authorities the flexibility to adjust it accordingly. In relation to the potential impact on customers, the EBA notes that this should be indeed captured in a scenario of significant disruption on the institution's ICT systems.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	Another respondent suggested including additional information on the quantification of ICT risk profile such as metrics and indicators (e.g. IT expenses/Total expenses, number of ICT service providers, records of ICT failures etc.).	The EBA deems the current level of information as sufficient to achieve a minimum level of harmonisation and at the same time maintain the principle of flexibility for the competent authorities.	No changes made.
3.2.2 Review of the critical ICT systems and services	A respondent proposed to specify the critical areas targeted during SREP and/or define clear criteria on determining critical ICT systems and services. Some other respondents were concerned that compliance with all the conditions described in Title 3.2.2 for identifying critical ICT systems and services could be quite burdensome, especially for cross-jurisdictional banks. They urged the EBA and the competent authorities to engage in a dialogue to achieve efficiencies in the workload arising from these Guidelines. Similarly, some other respondents noted the complexity and costs of assessing the risk controls on all systems and platforms, especially for institutions with global presence, and proposed the development of an engagement framework to avoid duplication across different regulatory jurisdictions.	Paragraph 40-41 in these Guidelines provide a number of conditions which could be used to define critical ICT systems and services. Business continuity, availability, security and confidentially perspectives could be used to identify critical ICT systems and services. The EBA also notes that the purpose of these Guidelines is not to provide detailed lists of criteria, controls and checks to be applied by the competent authorities but to specify a set of principle-based guidance that complement the EBA SREP Guidelines, in order to leave room for the application of the proportionality principle and preserve a level of supervisory judgement. The EBA wishes to clarify that the collection of information for groups and their entities should be duly coordinated in the college of supervisors.	Paragraph 19 has been added to clarify the use of college and other collaboration structures for authorities to leverage on existing information and to coordinate supervisory actions and requests to avoid duplication.
	Some respondents considered that the conditions listed in paragraph 39 (where at least one should be met for critical ICT systems and services) are quite broad resulting to a long list of critical ICT systems and services. It was also noted that reference to confidentiality would also expand the scope. The suggestion was to allow institutions to define their own criticality approach and rate/tier their critical ICT systems and services as these are structured along organisational and process-related multidimensional criteria. A proposal was made by one of	As previously mentioned, these Guidelines are addressed to the competent authorities as they provide a supervisory methodology for the assessment of ICT risks as part of the operational risk assessment in the SREP. Institutions should follow their own approaches for defining their critical ICT systems and services and this would be assessed as part of the SREP.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	the respondents to amend paragraph 39 to rephrase the sentence "**should** fulfil at least one of the following conditions" to "**could** fulfil at least one of the following conditions." As to not to make the principle too restrictive and instead to provide these as tools to help the identification of critical systems while not limiting it to this list.		
	It was further questioned whether the aforementioned list should be considered in addition to the BRRD and whether the Business Continuity Plan could be used as a starting point to identify the critical ICT systems and services.	The EBA acknowledges the common ground between critical ICT systems and services referred to in these Guidelines and "critical services" referred to in the BRRD. The former is deemed critical from the aspect of adequate functioning, availability, continuity and security of the institution's essential activities where the latter is determined based on whether they are needed to provide one or more critical functions. The latter is highly important in resolution planning and in the assessment of impediments to resolvability. Therefore, it is possible the former to be a subset of the latter in the context of BRRD.	No changes made.
3.2.3 Identification of material ICT risks to critical ICT systems and services	Clarification was requested by a respondent on whether the assessment of material ICT risks is linked to a qualitative assessment by the competent authorities. A respondent raised a concern about the fact that competent authorities would be determining materiality for ICT risks rather than the institutions and such an approach could lead to inconsistent interpretation of materiality across regulatory environments. This could create a significant challenge for institutions trying to comply consistently on a global or regional level.	As noted above, this guidance is addressed to the competent authorities with the view to establish consistent, efficient and effective supervisory practices. Moreover, the availability of assigned scores aims to bring a common supervisory methodology for assessing ICT risk and facilitate competent authorities in performing a high level transversal analysis of the position of the EU banking system with regard to ICT risks. The assessment of material risks could be based both on quantitative and qualitative assessment as well as to supervisory judgement.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		The EBA agrees on the importance of customer impact for determining potential impact of ICT risks on the critical ICT systems however this is deemed to be adequately captured in paragraph 43b.	No changes made.
	Some respondents pointed out that many Member States firstly focus on customer impact for determining system criticality and proposed adding a separate bullet point in paragraph 41 to highlight this. Another respondent suggested to exclude reference to the strategic impact on the institution referred to in point 41e – in the context of the potential impact of ICT risks – as this relates to business risk rather than operational risk.	A comprehensive assessment would need to be performed by the competent authorities to identify material ICT risks to critical ICT systems and services. It is noted that the purpose of this assessment is the identification of material ICT risks rather than their quantification. The EBA understands the concern for a possible overlap or double counting and notes that the application of the EBA SREP Guidelines in conjunction with these Guidelines should not result in double counting of capital requirements.	No changes made.
	One respondent indicated that the introduction in paragraph 42 of an obligation to map identified ICT risk categories that are considered material does not correspond with the initial statement that these Guidelines do not introduce any additional reporting. The respondent proposes to remove the obligation to map identified ICT risk categories. Another respondent asked for clarification that the mapping is not expected to be done by the institutions and proposes to rephrase paragraph 42 as follows: "The identified ICT risks that are considered material should then be mapped into the following ICT risk categories **by competent authorities, not by institutions**."	The requirement referred to in paragraph 44 for mapping the identified ICT risk categories is addressed to the competent authorities and not to the institutions and should therefore in itself not consist of any additional reporting obligation for institutions.	Paragraph 44 has been amended to clarify that the mapping needs to be done by competent authorities.
3.3 Assessment of the controls to mitigate material ICT risks	A respondent suggested it would be helpful to include a definition of controls.	The EBA refers to the definition of internal controls and control environment as embedded in the operational risk management principles of the	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		Basel Committee on Banking Supervision (BCBS).	
	Another respondent suggested clarifying further the practical use of principle of proportionality by stating that no separate processes for designing controls for mitigating material ICT risk would be necessary for small institutions with simple business structure as long as this risk is already adequately addressed by overarching operational risk controls.	The principle of proportionality applies throughout the Guidelines and it is not the intention to specifically restate it in different parts of the Guidelines.	No changes made.
3.3.1 ICT risk management policy, processes and tolerance thresholds	A respondent noted that further clarity on the tolerance thresholds would be useful, in particular clarifying whether a different tolerance threshold is expected for each ICT risk category.	In line with the proposed supervisory considerations for assigning an ICT risk score, tolerance thresholds should relate to the risk of potential significant prudential impact.	No changes made.
	Another respondent was concerned that setting ICT risk tolerance thresholds can be challenging as it is possible to miss alerts from "weak signals" analysis. Therefore, it was suggested to clarify that threshold would be only expected in few cases when relevant.	The EBA understands the difficulties on setting tolerance thresholds for risks and agrees on limiting this only in cases where relevant.	Paragraph 49d has been amended to incorporate relevance for tolerance thresholds.
	A respondent noted that the review of ICT risk management policies, processes and tolerance thresholds can be performed efficiently by referencing to an already reviewed enterprise-wide approach to operational risk rather than re-reviewing it as a distinct ICT risk management approach.	As mentioned in paragraph 49, ICT risk management policies, processes and tolerance thresholds can already be part of the operational risk assessment framework. The results of each institution's ICT risk profile review as well as the critical ICT systems and services review should inform competent authorities' decision on the ICT risk management approach.	No changes made.
	A respondent requested confirmation on whether the RCSA should be established by process and not by entities.	Competent authorities need to verify if a RCSA or similar process has been implemented. However competent authorities need to take into account this process might be organised at process level.	No changes made.
		Paragraph 49d refers to the existing ICT risk	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	Another respondent noted that point 49d on ICT risk management reporting may create an additional burden to institutions and introduce an additional internal reporting structure thus contradicting the Guidelines' intention for not introducing any additional reporting obligation.	management reporting of the institution, therefore no additional reporting obligations should be expected.	
	A respondent suggested adding ICT risk appetite and ICT risk tolerance definitions in order to highlight the differentiation between these two terms. COSO and ISO 31000 were referred to for the aforementioned definitions.	The EBA understands that the addition of other definitions may provide further clarity in some instances; however no value added can be seen by defining risk appetite and risk tolerance for ICT purposes. These should be considered to be in line with definitions set by the BCBS.	No changes made.
3.3.2 Organisational management and oversight framework	A respondent requested further information on how sufficiency of human resources will be assessed, proposing a case-by-case assessment given each bank's operating model.	Indeed, the competent authorities should assess whether the ICT risk management activities of the institution are performed by sufficient and quality human and technical resources. This assessment could be performed on a case-by-case basis given the business and operating model of each institution however benchmarking with peers could be also taken account in the final outcome.	No changes made.
	Some respondents suggested to add the materiality dimension rephrasing the narrative in paragraph 49e on the "exceptions from applicable ICT regulations and policies" to "exception from **risk-material** ICT regulations and policies" to specify it relates to technology policies such as the adoption of particular technology platforms.	The existing reference to "applicable ICT regulations and policies" is deemed to capture all ICT regulations and policies that are considered relevant to each institution.	No changes made.
	Another respondent suggested avoiding the quantification of ICT risks at the current time as this would require the use of new and unstable methodologies and lead to an additional burden for the	As mentioned above, these Guidelines are addressed to competent authorities and no new quantification methodologies are proposed either to the competent authorities or the institutions. It should be noted that quantification of material risks is implicit in the SREP Guidelines, where this is	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	institutions.	possible.	
3.3.4 ICT risk controls that are specific for the identified material ICT risks	A respondent suggested that Guidelines could mention that the level of risk severity of ICT systems and services cannot be assessed according to a single specific measurement but instead requires more orientation toward processes.	The EBA agrees that indeed a number of factors should be taken into account for assessing the risk severity of ICT systems and services rather than only a single specific measurement.	No changes made.
	A respondent suggested that data integrity requirements should be more flexible than for the definition of a framework as this would depend on the risk assessment of each institution.	The EBA notes that expectations have been articulated at a sufficient level with the existing references to ICT data integrity risk providing adequate flexibility to the competent authorities for properly assessing the ICT data integrity risk.	No changes made.
	A respondent noted that it is often difficult to evaluate controls for the proper assessment of ICT outsourcing risks. It was suggested to specify in more detail expectations from internal (intragroup) and external service providers and also add further details on cloud service providers.	The appropriateness and effectiveness of each institution's outsourcing strategy and risk framework should be part of the assessment of controls for managing ICT outsourcing risks as proposed in these Guidelines. In line with the CEBS Outsourcing Guidelines, it should be noted that neither intragroup nor external outsourcing is risk free. Supervisory expectations would depend to the risks presented by any outsourcing arrangements. EBA is also undertaking additional work on harmonised requirements for institutions outsourcing to cloud service providers.	No changes made.
	Another respondent suggested including a mapping table between the ICT risk categories and protection targets/standards so as to improve transparency.	The EBA understands the possible use of such a mapping however it may undermine the spirit of flexibility and proportionality of these Guidelines. In addition, it is not clear how such a mapping could facilitate the ICT risk assessment performed by the competent authorities.	No changes made.
(a) Controls for	Some respondents suggested to amend the reference to	The EBA wishes to clarify that the existing	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
managing material ICT availability and continuity risks	"a comprehensive analysis of dependencies between the critical business processes" in paragraph 52a(i) with "a mapping between critical business processes and supporting systems" as the existing reference suggests a dynamically updated CMDB.	reference does not suggest a dynamically updated CMDB but rather for the ICT availability and continuity risk management framework to sufficiently identify the supporting systems which are directly linked to the critical business processes (from a business resilience and continuity plans perspective) in such a way which creates dependencies to those supporting systems.	
	Some respondents proposed to add in paragraph 52b(i) relevant reference for the sufficient separation between data centres i.e. not limited to geographical separation but also to suppliers' separation.	The EBA welcomes the proposed addition and notes that indeed a number of measures should be included in the business resilience, continuity control environment policies and standards and operational controls to avoid adverse impact to both ICT production and recovery systems.	Paragraph 54b(i) has been amended to refer to measures more broadly, and not only physical separation of data centres.
	Some respondent suggested to clarify that monitoring of ICT availability or continuity incidents referred to in paragraph 54b(iii) should be subject to system criticality and other risk considerations as it is currently suggesting to cover all elements of ICT solutions across the institution. In addition, another respondent suggested to replace the term *solution* presented in paragraph 52b(iii) with *processes for critical applications* so as to clarify that this requirement applies to critical applications.	The EBA wishes to clarify that the overall principle of proportionality applies throughout the Guidelines and systems criticality and other factors, as these are outlined within the Guidelines, should be taken into account for the ICT availability and continuity risk assessment.	No changes made.
	Some respondents suggested that there should be a difference between in-house systems and outsourced solutions in paragraph 52b as there are no known operational controls for outsourced solutions. It was noted that banks always retain the ultimate responsibility and suggested that these Guidelines can be used to	As mentioned above, these Guidelines should be considered in line with the CEBS Outsourcing Guidelines where both external and internal service providers are captured under the definition of outsourcing.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	improve the operational controls of outsourced solutions by third parties.		
	A respondent suggested clarifying that the term *incident management* referred to in paragraph 52b(iv) does not necessarily refer to the ITIL *incident management process* and that the use of ITIL terminology does not result in additional requirements.	The EBA wishes to clarify that unless explicitly specified in the Guidelines the terminologies used across the document do not refer to any IT technical standards, IT libraries or glossaries.	No changes made.
	Some respondents suggested to adopt a wider view of cyber threats through paragraph 52b(ix) rather than limiting it to DDOS attacks. In addition, a level of duplication was noted with paragraph 52b(v) which refers to cyber-attacks.	The EBA welcomes the suggestions and agrees with both the adoption of a wider view of cyber-attacks and the observation of a possible duplication.	Point 54b(v) has been removed and point 54b(viii) has been amended to include other cyber-attacks.
	A few respondents suggested referring to expected and proven recoverability in paragraph 52c rather than the need for back-ups to reflect current thinking on ICT resilience. It was further suggested that scenario-based plans need to identify critical resources and then assess how the lack of such resources can be managed.	Paragraph 54c refers to a range of realistic scenarios which could be used to test ICT availability and continuity solutions. Cyber-attacks and tests of back-ups for critical software and data are provided as examples of realistic scenarios and do not intend to limit the range of realistic scenarios as competent authorities may consider different scenarios for each institution. Nevertheless, the EBA welcomes the suggestions and agrees to include the integrity dimension.	Paragraph 54c has been amended to include fail-over tests.
(b) Controls for managing material ICT security risks	A respondent noted that ISO 27015 was withdrawn by ISO JTC1-SC27 in October 2016.	The EBA welcomes the correction and deems appropriate to remove references to specific international standards.	The ISO reference in paragraph 55b has been removed.
	A respondent commented that the vulnerability	The EBA does not consider that additional clarifications/comments are required on this	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	assessment results (referred to in paragraph 53a(iii)) are part of the daily operational business with known vulnerabilities fed into incident and patch management processes. A process/assessment through the obligatory risk management processes becomes necessary only for unresolved vulnerabilities.	reference as the vulnerability assessment process is provided as an example for protecting the critical ICT systems and services.	
	A respondent noted that logging possibilities are also subject to legal and regulatory requirements related to personal data, banking secrecy and data location etc. Therefore, it was suggested to amend accordingly point 53e.	Paragraph 55e refers to the adequacy of logs and it is not deemed to contradict or be subject to any specific legal or regulatory requirement. To this end, the EBA does not consider the proposed reference as applicable.	No changes made.
	A respondent suggested rephrasing paragraph 53 to include the possibility for the competent authorities to rely on an external auditor's report on ICT security risk, if any, rather than performing a full assessment on the ICT security risk control framework.	While competent authorities can always choose to build on work conducted at institutions by external auditors, they retain the right to perform their own examinations.	No changes made.
(c) Controls for managing material ICT change risks	Some respondents noted that paragraph 54b does not seem to allow for the adoption of continuous or agile delivery in case where functions of developer and operator are combined to a degree but within more highly controlled tools and back-out approaches.	As previously mentioned, these Guidelines are addressed to the competent authorities and do not intend to provide detailed requirements to institutions in managing ICT change risks.	No changes made.
	Some respondents proposed to extend paragraph 54c (test environments that adequately reflect production environments) for better reflecting the criticality of a system for replication in a test environment and the wider role of quickly deploying and backing-out changes rather than undergoing extensive proving in non-production environments.	The EBA welcomes the suggestion and considers the existing reference to be sufficient and adequate for assessing the institution's ICT change risk management framework. Nevertheless, it is noted that the proposed list of controls should not be considered exhaustive as it provides the competent authorities with the flexibility to consider other controls in their assessment.	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	Some respondents suggested that paragraph 54g should consider both the risk of the change as defined by the institution but also that security vulnerabilities can be exploited in non-internet facing software.	The EBA welcomes the suggestion and agrees that process to conduct a security and vulnerability screening should not be limited only to internet facing software.	Paragraph 56g has been amended to broaden the scope to all new or materially modified ICT systems and software.
	A respondent suggested removing reference to *test and development environment* in paragraph 54d as no asset inventory is maintained for the test and development environment.	The EBA wishes to clarify that asset inventory for the test and development environment should not be seen only in the context of CMDB, therefore to avoid any possible confusion the aforementioned reference/example has been removed. However, the inventory needs to be kept for all environments.	Paragraph 56d has been amended to remove the reference to the CMDB database.
	A respondent suggested specifying in paragraph 54e that the management and monitoring process for the life cycle of the used ICT systems should apply only to the *critical* ICT systems. It was further suggested amending the aforementioned paragraph to clarify that ICT solutions can be also supported by the institution itself rather than only by vendors and rephrase paragraph 54e to "and to make sure that the used ICT solutions and systems are still supported by their vendors **or by the institutions itself**."	The EBA wishes to clarify that the overall principle of proportionality applies throughout the Guidelines and systems critically and other factors, as these are outlined within the Guidelines, should be taken into account for the ICT change risk assessment. Moreover, institutions' own ICT solutions and systems are considered to be kept by the institutions themselves therefore such a process should be seen as more applicable to cases where used ICT solutions and systems are supplied by vendors.	No changes made.
(d) Controls for managing material ICT data integrity risks	Further guidance was requested in relation to the assessment of institutions' risk reporting and data aggregation capabilities compared to the BCBS 239 principles for effective risk data aggregation and risk reporting, and to include further illustrations of the envisioned assessment criteria in paragraph 56 which	The EBA appreciates this suggestion however the scope and mandate of these Guidelines do not include providing clarifications on the BCBS 239 principles. As regards the assessment criteria, the EBA notes that the proposed list of controls and guidance provide competent authorities with a	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	mentions the link to RDA. It was also recommended that a more risk-based approach should be adopted in terms of managing ICT data integrity risks as the existing requirements in paragraph 55a and 55b widen the scope of several BCBS 239 requirements.	sufficient framework on performing ICT data integrity risk assessment preserving at the same time the principle of flexibility. The EBA wishes to clarify that the scope of these Guidelines is wider than risk data as defined under BCBS 239.	
	Another respondent highlighted the appropriateness of established mechanisms to assure data quality and argued that focusing on the perceived need to create organisational structures for this end would not significantly contribute to this objective. In addition, this approach could undermine the efficiency of institutions by creating structures that may not be effective according to their size.	The EBA welcomes the comments on data quality management and wishes to note that the proposed list of controls and guidance provided to the competent authorities on ICT data integrity risk assessment should not be perceived as exhaustive in the spirit of preserving the principle of flexibility.	No changes made.
(e) Controls for managing material ICT outsourcing risks	Several respondents suggested differentiating the ICT intra-group outsourcing risk as different risks may arise from outsourcing with third parties and intra-group outsourcing. In particular, the following addition was suggested to paragraph 57: "when assessing ICT intra-group outsourcing risk, competent authorities should adapt the assessment adequately". It was further noted that a number of benefits are provided from intra-group outsourcing and these may disappear if same requirements are applied to both outsourcing categories. In addition, it was noted that control over outsourced solutions has to be on a higher level than on outsourced systems.	These Guidelines do not intend to minimise or restrict any benefits from intra-group outsourcing agreements. The ICT outsourcing risk definition as presented in these Guidelines captures both outsourcing with third parties and intra-group outsourcing. In line with the CEBS Guidelines on Outsourcing, competent authorities may take specific circumstances into consideration when assessing the risks associated with an intragroup outsourcing arrangement and the treatment to apply to such arrangements. In addition, institutions should recognise that no form of outsourcing is risk free and that the management of intra-group outsourcing should be proportionate to the risks presented by these arrangements.	No changes.
	Some respondents indicated that the phrase "mitigating	The EBA welcomes the proposed correction and	Paragraph 60 has been amended to

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	material outsourced ICT services" in paragraph 58 should relate to the outsourced ICT "risks" rather than "services".	proceeded with the necessary amendment.	refer to "risks related to material outsourced ICT services."
3.4 Summary of findings and scoring			
Supervisory considerations for assigning an ICT score	Some respondents suggested the revision of the risk scoring table by taking into account a combination of potential losses (severity) and probability of occurrence (frequency) rather than focusing only on the number of potential risks.	These Guidelines mainly feed into and complement the existing ICT risk assessment component of the EBA SREP Guidelines, under Operational Risk (Section 6.4) under Title 6 – Assessing risks to capital. Table 1 in these Guidelines should be considered by competent authorities when assigning the score of operational risk in Table 6 of the EBA SREP Guidelines.	No changes made.
Use of risk scoring methodology	A respondent suggested that the risk scoring methodology should be used by institutions that do not have an existing risk scoring methodology.	The purpose of the risk scoring table is to facilitate competent authorities' assessment for operational risk in the context of SREP in forming an opinion on the institutions' ICT risks rather than to be used by institutions themselves.	No changes made.
	Another respondent suggested providing further information on the assignment of ICT risk score by competent authorities in terms of the ICT risk taxonomy.	The EBA wishes to note that these Guidelines should be read along with the EBA SREP Guidelines as should be seen as a supplement to them. To this end, the same level of detail has been used for the development of these Guidelines in relation to the assignment or risk scores taking also into account the need to preserve both proportionality and flexibility principles.	No changes made.
Annex - ICT Risk Taxonomy			
Common Taxonomy	Several respondents proposed to make reference to a common taxonomy in the Guidelines (such as	The EBA wishes to clarify that institutions are expected to maintain their own risk taxonomies for	Paragraph 18 has been amended to

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	COBIT/Basel/ISO 27000) underlining at the same time the importance for institutions to have the flexibility to manage risks using their own taxonomies. Similarly, a number of respondents requested confirmation on whether institutions should need to adjust their internal taxonomies to align with the ICT risk taxonomy proposed by these Guidelines. A respondent proposed to include reference to a common taxonomy that takes into consideration best practices and appropriately includes definitions for cyber risk, leaving at the same time flexibility in implementation.	risk management purposes as the ICT risk taxonomy set out in the Annex is intended to be used as guidance for the competent authorities during the SREP exercise.	clarify that institutions are expected to maintain their own risk taxonomies.
Map events to risk categories	Many respondents observed overlaps in the proposed ICT Risk Taxonomy, and mixing up of causes, events and consequences. A number of respondents noted that the proposed risk drivers under the five definitions are not complementary to each other leading to overlaps and causing undesirable risk attributions issues (i.e. an event could be mapped to more than one risk category). Therefore, further clarifications were asked in terms of interpreting the taxonomy so as to correctly allocate events to ICT risk categories.	As mentioned above, these Guidelines are addressed to the competent authorities and the proposed risk taxonomy aims to bring about a uniform understanding of risk categories and facilitate a common language with a non-exhaustive list of risks under each category with descriptions and examples. The proposed risk categories under ICT risks are not exhaustive allowing competent authorities the flexibility to consider other ICT risks in their assessment.	No changes made.
	Some respondents commented that taxonomy elements correspond mainly to ICT processes/causes rather than to risks. Specifically, it was suggested that ICT risks mapped to ICT change risk and ICT outsourcing risk are causes of three principle risks, namely confidentiality, integrity or availability. It was also noted that some ICT risks may be reported in other Basel event types (e.g. cyber-attack often materialises through fraud events). Same respondents proposed that risk categories should be mutually exclusive to facilitate reporting and assessments and suggested ICT risk categories to be renamed and limited to four complemented by causes	The EBA acknowledges possible overlaps in the ICT risk taxonomy table and wishes to clarify that the intention of the taxonomy is not to present a one-to-one mapping of risk events and ICT risk categories nor to provide a fully mutually exclusive taxonomy, but to establish a link between the more IT technical concepts and concerns and the main ICT risks to capital. The EBA also notes that the ICT risks presented in the taxonomy are listed under the risk category they most impact but it is possible to impact other risk categories too. Additionally, this taxonomy enhances the	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
	and risk drivers: ICT unavailability, ICT security, ICT data integrity and ICT project failure. Another respondent suggested providing further guidance for mapping ICT risks to the proposed ICT risk categories presented in the Annex. Some respondents questioned whether the EBA intends to provide a mapping of this ICT risk taxonomy with the operational risk framework (as per the Basel II classification logic) or each institution should prepare its own mapping. One respondent proposed an alternative categorisation while several respondents indicated that risks should be defined by events, ICT failure as a cause should be identified, and that reporting on ICT should be a mix of ICT events and events with an ICT cause.	convergence in the assessment of ICT risks as these risks are, by their nature, cross -border and there is a need to have a common understanding among competent authorities across Member States.	
ICT availability and continuity risks	Some respondents suggested that this risk category should also give prominence to the design and operation of resilient systems by including automatic resilience, reduction in manual processes, monitoring etc.	The EBA welcomes the comment and notes that the design and operation of a resilient system is already covered under the ICT availability and continuity risks. As it follows from the definition of ICT availability and continuity risk, the design and operation of resilient systems will directly affect the performance and availability of ICT systems. The list of ICT risks proposed in the Annex is non-exhaustive and can be adjusted accordingly by competent authorities.	No changes made.
ICT outsourcing risk category	Another suggestion was the separation of the ICT consequences arising from the activities of the service provider (which should be linked to the remaining 4 ICT risks) and the risks derived from the choice and management of that service provider.	In line with the ICT outsourcing risk definition set out in these Guidelines, the ICT outsourcing risk category captures the risk arises from engaging with an outsourcing service provider (as defined in the CEBS Outsourcing Guidelines). Both cases proposed should be captured within the aforementioned definition. As already mentioned	No changes made.

Comments	Summary of responses received	EBA analysis	Amendments to the proposals
		in the Annex, the list of ICT risks proposed is non-exhaustive therefore it can be adjusted accordingly by competent authorities.	
ICT change risk category	A respondent noted that risks presented under this category are more causes which could result in ICT availability, security or integrity issues.	The EBA welcomes the comment and notes that the ICT risks presented in the taxonomy are listed under the risk category they most impact but it is possible to impact other risk categories as well.	No changes made.
ICT data integrity risk category	A respondent proposed to clarify that this category targets unintended situation with intended situation being captured under the ICT security risk.	The EBA acknowledges the suggestion and wishes to clarify that the ICT security risk definition is deemed to cover both intentional and unintentional unauthorised access to ICT systems.	No changes made.
ICT security risk	One respondent pointed out that the definition of ICT security risks in paragraph 9 is not consistent with ICT security risk as it is described in the Annex. Some of the details included in the Annex have nothing to do with "unauthorized access". For instance, for DDoS there is no kind of "unauthorized access" to your systems.	As per the Annex of the Guidelines, DDoS attacks are mapped to the "disruptive and destructive cyber-attacks" risk which then rolls up to the ICT availability and continuity risks.	No changes made.
	Some respondents questioned how this section can be kept updated and respond to emerging threats and approaches.	The EBA as well as the competent authorities will be revisiting these Guidelines if and when deemed necessary depending on the observed evolutions and developments in the ICT environment.	No changes made.