EBA/CP/2016/14

06/10/2016

Consultation Paper

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

Contents

1. Responding to this consultation

The EBA invites comments on all proposals put forward in this paper.

Comments are most helpful if they:

- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices the EBA should consider.

Submission of responses

To submit your comments, click on the ‘send your comments’ button on the consultation page by 06.01.2017. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

Please clearly indicate in the consultation form if you wish your comments to be disclosed or to be treated as confidential. A confidential response may be requested from us in accordance with the EBA’s rules on public access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the EBA’s Board of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the EBA is based on Regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December 2000 as implemented by the EBA in its implementing rules adopted by its Management Board. Further information on data protection can be found under the Legal notice section of the EBA website.

2. 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 et seq. of Directive 2013/36/EU[1]. In particular, these guidelines further specify the treatment of risk under Article 76 of Directive 2013/36/EU in relation to institution-wide ICT risks and the assessment of ICT risk as a component of operational risk under Article 85 of Directive 2013/36/EU.

These guidelines are designed to supplement and further specify the EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) (EBA/GL/2014/13) (from here on 'EBA SREP guidelines'), in particular building on paragraphs 258-261 thereof, and should be read along with the EBA SREP guidelines. Competent authorities should therefore ensure that the EBA SREP guidelines remain applicable as appropriate.

These guidelines apply to all institutions in line with the level of application as set out in the EBA SREP guidelines. However, 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.

The requirements to assess ICT risk as set out in these guidelines consist of the following three parts:

Title 1 - general provisions;

Title 2 - assessment of institutions' governance and strategy on ICT; and

Title 3 - assessment of institutions' ICT risk exposures and controls.

The ICT risk assessment contribute to the overall SREP assessment as follows: the assessment of institutions' governance and strategy on ICT (Title 2) feeds into the assessment of internal governance and institution-wide controls under Title 5 of the EBA SREP guidelines and is intended to form part of the score included in the same Title as well as potentially informing the assessment of the business model assessment under Title 4 of the EBA SREP guidelines. The assessment of ICT risk (Title 3) results in a summary of findings which, based on a set of considerations at the end of Title 3 of these guidelines, will inform the Operational Risk score of the EBA SREP guidelines - part of the assessment of 'Risks to capital' in Title 6 of the EBA SREP guidelines. Additionally it should be noted that the outcome of the assessment in

[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, p 338.

Title 2 should inform, where relevant, the assessment of risk management and controls in Title 3 of these guidelines.

In accordance with paragraph 116 of the EBA SREP guidelines sub-categories of risks can be assessed and scored individually, when they are deemed material. Therefore, should ICT risk be identified as a material risk by the competent authority, the scoring table at the end of Title 3 of these guidelines should be used to provide a stand-alone sub-category score on a scale of 1-4, which is in accordance with the common SREP scoring methodology, for this Operational sub-category risk.

Title 1 of these guidelines provides the General provisions for applying these 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. 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; as highlighted in the EBA SREP guidelines (paragraphs 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 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).

These guidelines are complemented by an ICT risk taxonomy in the annex which includes a list of 5 ICT risk categories 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.

3. Background and rationale

In accordance with Article 16 of Regulation (EU) No 1093/2010[2] ('the EBA Regulation'), the EBA shall issue guidelines addressed to competent authorities, with a view to establishing consistent, efficient and effective supervisory practices and ensuring the common, uniform and consistent application of European Union law.

In addition, Article 107 (3) of Directive 2013/36/EU ('CRD') mandates the EBA to draw up guidelines for competent authorities on the common procedures and methodologies for the SREP and for the assessment of the organisation and treatment of the risks referred to in Articles 76-78 of that Directive. These guidelines on ICT risk assessment complement the existing EBA SREP guidelines, in particular paragraphs 258-261 thereof, and they provide a supervisory methodology for the assessment of ICT risk as part of Operational Risk under Article 85 of the CRD as part of the SREP and further specify the treatment of risks under Article 76 of the CRD in relation to ICT risk.

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.

As these guidelines build on existing references to ICT risk in the SREP guidelines and also feed into the SREP methodology more generally, the EBA SREP guidelines remain applicable as appropriate. This is the case for, inter alia, the proportionate way the methodology contained within these guidelines should be applied including using the categorisation criteria and minimum supervisory engagement level described in the EBA SREP guidelines paragraphs 36-42, the addressees of these guidelines and the level of application. In line with the principle of proportionality and the minimum engagement model explained in Section 2.4 of the EBA SREP guidelines, the use of supervisory judgement is required in deciding to what extent the guidelines should be applied as these guidelines apply to all categories of institutions as explained in Section 2.4 of the EBA SREP guidelines (4 categories of institutions). This means that the depth and detail of the ICT risk assessment should be conducted in a manner that is proportionate to the size, structure and operational environment of the institution as well as the nature, scale and complexity of their activities.

As mentioned above, 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. 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 expect to see 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 in Title 5 of the EBA SREP guidelines. Finally these guidelines also include assessment of an institution's ICT strategy and the alignment with the institution's business strategy which can affect the business model assessment under Title 3 of the EBA SREP guidelines.

[2] Regulation of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), OJ L 331, 15.12.2010, p. 12

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:

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

Acknowledging the growing importance of ICT systems and hence the increasing potential adverse prudential impact from failures on an institution and on the sector as a whole (due to the cross-border nature of this risk), and taking into account the technical specificities of ICT risk assessments and the objective to harmonise the existing ICT supervisory risks assessments within the EEA, these guidelines provide guidance to supervisors for assessing ICT risk in institutions. They supplement the existing limited information in the EBA SREP guidelines on how to assess ICT risk and harmonising the methodology for doing so. In addition to bringing about a common supervisory methodology for assessing ICT risk, the availability of assigned scores will make it possible for competent authorities to perform a high level transversal analysis of the position of the EU banking system with regard to ICT risks.

These guidelines are aimed at addressing risks arising to market integrity and the financial viability of credit 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.

Additionally the focus of these guidelines is on the ICT dimensions of the risk management processes covered in these guidelines and does not look at 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 any additional reporting obligation 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.

4. Draft EBA Guidelines on ICT risk under the Supervisory Review and Evaluation process

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/201x/xx'. 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 further specify the common procedures and methodologies for the supervisory review and evaluation process (SREP) referred to Article 97 of Directive 2013/36/EU[5] in relation to Information and Communication Technology (ICT) risks and apply to:

a) the supervisory assessment of institutions' governance and strategy on ICT; and

b) the supervisory assessment of institutions' ICT risk exposures and controls.

6. These guidelines complement and further specify the EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) (EBA/GL/2014/13) (from here on 'EBA SREP guidelines'), in particular the assessment referred to in paragraph 5a) above and as set out in Title 2 supplements Title 5 of EBA SREP guidelines and informs, where applicable, the business model assessment under Title 4 of the EBA SREP guidelines; the assessment referred to paragraph 5b) above and as set out in Title 3 further specifies the Operational Risk assessment contained within Title 6.4 of the EBA SREP guidelines.

7. Competent authorities should apply these guidelines in line with the EBA SREP Guidelines.

Addressees

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

Definitions

9. 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 working together as part of a mechanism or an interconnecting network that support the operations of an institution.

[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, p 338.

ICT services

Services provided by ICT systems to one or more internal or external users. Examples include data entry, data storage, data 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 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

These guidelines apply from dd.mm.yyyy [Date of application usually 6 months after date of publication]

4. Requirements for the ICT Risk Assessment

Title 1 - General provisions

Level of application

10. In accordance with paragraph 4 et seq. of the EBA SREP guidelines the requirements set out in these guidelines should be applied to all institutions in line with the level of application as set out therein.

Proportionality

11. Competent authorities should apply these guidelines in a manner proportionate to the size, structure and operational environment of institutions as well as the nature, scale and complexity of their activities. 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. In accordance with Title 2, Section 2.4 of the EBA SREP guidelines, competent authorities should apply these guidelines in line with the frequency and intensity as per the categorisation of institutions as set out therein. In conducting the assessment contained within these guidelines, competent authorities should rely on the minimum level of engagement as specified in the aforementioned section of the EBA SREP guidelines.

13. Competent authorities may rely on and take into consideration work already undertaken by the institution or by the competent authority in the context of other risk assessments in order to have an update of the assessment in line with the categorisation of the institution. Specifically, in conducting the assessments contained 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.

Use of findings and scoring

14. In the context of concluding the assessment in these guidelines, the assessment under Title 2 of these guidelines should result in findings that inform the summary of findings under Title 5 of the EBA SREP guidelines and the respective scoring in line with the considerations in Table 3 of the EBA SREP Guidelines. 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 assessment of Title 4 of the EBA SREP guidelines. In relation to the outcome of the assessment of ICT risk in Title 3 of these guidelines, the findings from the assessment should feed into the summary of findings of Operational Risk and should be considered as informing the subsequent score in Table 6 of the common SREP guidelines.

15. Where competent authorities deem ICT risk to be material and decide to assess and score this risk individually as a sub-category of Operational Risk in line with paragraph 116 et seq. of the EBA SREP guidelines, the scoring table (Table 1) in these guidelines ('Supervisory considerations for assigning an ICT risk score') should be used to reach a score.

16. 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 list of sources in paragraph 120 of the EBA SREP guidelines to assist in identifying whether ICT risk is material.

17. 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.

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

2.1 General principles

18.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.

19.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) and international guidance in this field, to the extent these are applicable given the specificity of ICT systems and risks.

20.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.

21.Point a) referred to in paragraph 20, 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.

22.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

23.Under this section competent authorities should assess whether the ICT strategy is subject to adequate oversight from the institution's management body, whether the institution has an ICT strategy in place that: is consistent with the business strategy, particularly for keeping its ICT up-to-date and planning or implementing important and complex ICT changes; and supports the institution's business model.

2.2.1 ICT strategy development and adequacy

24. 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. senior business management is adequately involved in the definition of the institution's strategic ICT priorities and that, in turn, senior ICT management 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

25. 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 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

26. 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;

27. Further to paragraph 85 (d) 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

28. 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.

29. 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.

30. 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

31. 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.

32. 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

33. 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.

34. 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.

35. 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 (e.g. 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

36. 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

37. 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 35 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

38.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.

39.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

40. 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.

41. 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.

42. The identified ICT risks that are considered material should then be mapped 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

43. 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.

44. 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.

45. 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 common 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 35 of these guidelines.

46. 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

47. 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 and to monitor changes of material ICT risks..

3.3.2 Organisational management and oversight framework

48. 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

49. 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

50. 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

51. 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.

52. 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. Sufficient distance between ICT production and the recovery systems with to avoid that both might be impacted by the same incident or disaster;

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. plans and solutions for the IT continuity and availability risks that may be generated by possible cyber-attacks;

vi. 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);

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

viii. 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;

ix. solutions to protect critical internet activities or services (e.g. e-banking services), where necessary and appropriate, against denial of service 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 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

53. 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 (e.g. ISO 27001 and ISO 27015) 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. datacenters);

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

54. 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 (e.g. a configuration management data base 'CMDB') 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 internet facing 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

55.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[6], data custodians[7], data owners/stewards) 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…) 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.

56.For supervised institutions that fall under the scope of the BCBS 239 principles for effective risk data aggregation and risk reporting, competent authorities should review the institution's risk analysis of its

[6] A data officer is responsible for data processing and usage.

[7] A data custodian is responsible for the safe custody, transport and storage of data.

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

57.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.

58.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 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.

.

3.4 Summary of findings and scoring

59.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.

60. 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 35 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. .	• The institution’s ICT risk policy and strategy is commensurate with its overall strategy and risk appetite.
2	There is a low risk of significant prudential impact on the institution considering the level of inherent risk and the management	• The information sources to be considered under paragraph 35 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	

	and controls.	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 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 35 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 35 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[8])	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.

[8] 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[8])	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 security	Gaining unauthorised access to critical ICT systems from within the institution for different purposes (e.g. fraud, performing and hiding rogue trading activities,	• Installing key stroke loggers (key loggers) to steal user IDs and passwords to gain unauthorised access to confidential data and/or commit fraud.

ICT risk categories	ICT risks (non exhaustive[8])	Risk description	Examples
		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).	• 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 caused by terrorism, accidents or unfortunate/erroneous manipulations by staff of the	• Physical terrorism (i.e. terrorist bombs) or sabotage of ICT assets. • Destruction of data centre caused by fire, water

ICT risk categories	ICT risks (non exhaustive[8])	Risk description	Examples
		institution and/or third parties (suppliers, repairman).	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 commercial software packages with internally developed software, leading to the incapacity to implement future releases and upgrades of the

ICT risk categories	ICT risks (non exhaustive[8])	Risk description	Examples
			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 models or data dictionaries	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 models or data definitions, and/or differences in the underlying data generation and change process.	• 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 the level of the whole financial institution or group.
ICT outsourcing	Inadequate resilience of third	The non-availability of critical outsourced ICT services, telecommunication services and utilities.	• Unavailability of core services as a result of failures in suppliers (outsourced) ICT systems or

ICT risk categories	ICT risks (non exhaustive[8])	Risk description	Examples
risks	party or another Group entity services	Loss or corruption of critical/sensitive data entrusted to the service provider	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.

4 Accompanying documents

4.1 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 draft 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 draft 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.

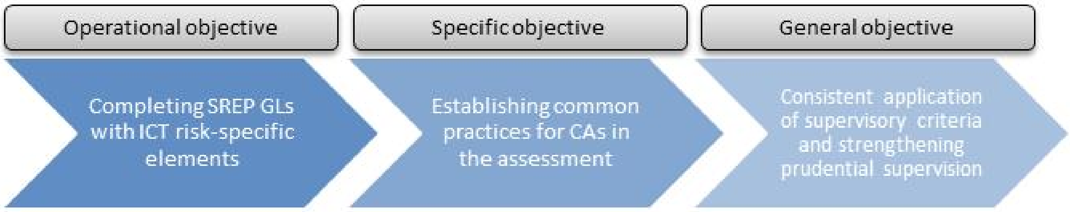
The core gap that the current draft guidelines aim to address is the lack of in depth guidance for the supervisory assessment of ICT risk in institutions and therefore room for lack of assessment of this risk, as well as inconsistency in assessing ICT risk across MS leading to a lack of comparability 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 draft 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 draft 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 current draft guidelines:


Operational objective
Specific objective
General objective
Completing SREP GLs with ICT risk-specific elements
Establishing common practices for CAs in the assessment
Consistent application of supervisory criteria and strengthening prudential supervision

C. Baseline scenario

Table 1 presents the baseline scenario by Member State on the 'compliance' of the institutions and the competent authorities with these draft guidelines. Precisely, it presents in each Member State an overview of current implementation and practices in relation to the major sections of the draft 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 draft 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 draft guidelines, the practices of some other Member States (AT, BE) do not show similarities with these provisions. On average, the current practices in Member States mostly cover the provisions of the draft guidelines. Table 2 shows the implementation level indicated by the Member States in percentage terms. In terms of the sections of the draft guidelines except two sections[9] of the draft 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.

[9] 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 draft guidelines, by Member State

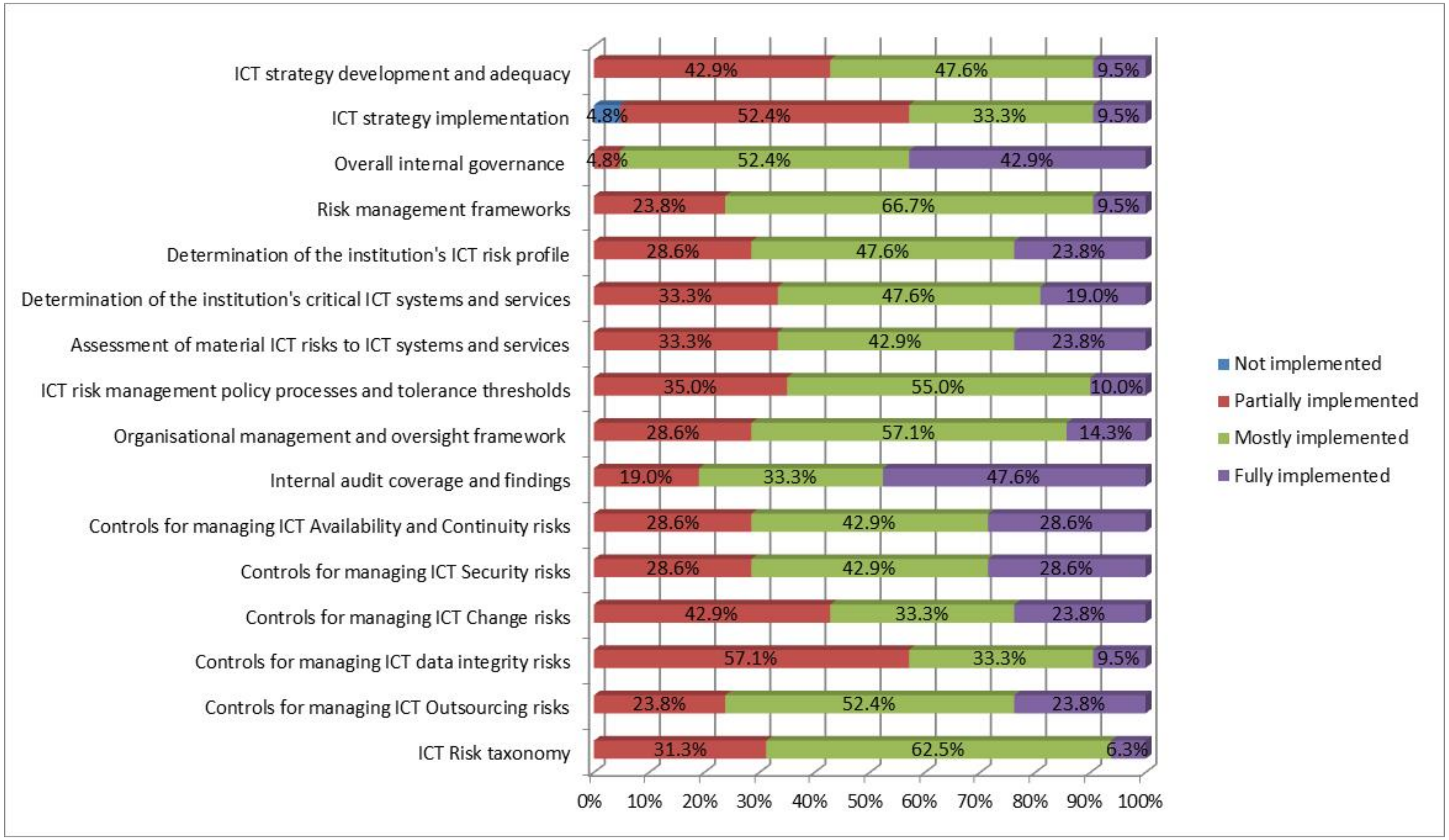
	Title 2				Section 3.2			Section 3.3.								Annex
	2.2.1 ICT strategy development and adequacy	**2.2.2 ICT strategy implementation**	**2.3 Overall Internal Governance**	**2.4 Risk management frameworks**	**3.2.1 Determination of the institution’s ICT risk profile**	**3.2.2 Determination of the institution's 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	2	2	3	2	2	2	2	2	2	2	2	2	2	1	2	2

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

‘:’ = not ranked

Table 2 Current practices with respect to the content of the draft 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 draft 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 draft 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 draft 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 draft 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 draft 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 draft guidelines. Potential sources of additional costs for institutions in the implementation of the draft 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 draft 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 draft 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 draft 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 draft guidelines.

ICT is a crucial element of modern banking services with a significant impact on the institution's competitiveness and cost effectiveness. The draft guidelines help draw a sound framework for better management of ICT risk and other ICT practices within the institutions. The draft 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 draft 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 draft guidelines.