BANCO DE ESPAÑA
Eurosistema

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

(EBA/GL/2017/05)

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

These Guidelines aim to ensure the convergence of supervisory practices in the assessment of the Information and Communication Technology (ICT) risk under the supervisory review and evaluation process (SREP) referred to in Article 97 of Directive 2013/36/EU. In particular these Guidelines specify the assessment criteria that competent authorities should apply in the supervisory assessment of institutions' governance and strategy on ICT and the supervisory assessment of institutions' ICT risk exposures and controls.

Competent authorities should apply these Guidelines in line with the level of application of SREP specified in the EBA SREP Guidelines and in accordance with the proportionality principle established therein.

These Guidelines have been developed on the EBA's own initiative in accordance with article 16 of Regulation (EU) No 1093/2010. The European Banking Authority published the English version of these Guidelines on 11 May 2017 (the Spanish version was released on 11 September 2017). The Guidelines will apply from 1 January 2018.

Banco de España's Executive Commission, in its role of competent authority for the direct supervision of the less significant institutions, adopted these Guidelines as their own on 07.11.2018.

EBA/GL/2017/05

11/09/2017

Guidelines

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

1. Compliance and reporting obligations

Status of these Guidelines

1. This document contains Guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010[1]. 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 13.11.2017 In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website to compliance@eba.europa.eu with the reference 'Eba/gl/2017/05. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to EBA.

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

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

2. Subject matter, scope and definitions

Subject matter and scope of application

5. These Guidelines, drawn up pursuant to Article 107(3) of Directive 2013/36/EU[2] aim to ensure the convergence of supervisory practices in the assessment of the information and communication technology (ICT) risk under the supervisory review and evaluation process (SREP) referred to in Article 97 of Directive 2013/36/EU and further specified in the EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP)[3]. In particular these Guidelines specify the assessment criteria that competent authorities should apply in the supervisory assessment of institutions' governance and strategy on ICT and the supervisory assessment of institutions' ICT risk exposures and controls. These Guidelines form an integral part of the EBA SREP Guidelines.

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

Addressees

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

Definitions

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

ICT systems

ICT set-up as part of a mechanism or an interconnecting network that support the operations of an institution.

ICT services

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

[2] 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.

[3] EBA/GL/2014/13

processing and reporting services, but also monitoring, business and decision support services.

ICT availability and continuity risk

The risk that performance and availability of ICT systems and data are adversely impacted, including the inability to timely recover the institution’s services, due to a failure of ICT hardware or software components; weaknesses in ICT system management; or any other event, as further elaborated in the Annex.

ICT security risk

The risk of unauthorised access to ICT systems and data from within or outside the institution (e.g. cyber-attacks), as further elaborated in the Annex.

ICT change risk

The risk arising from the inability of the institution to manage ICT system changes in a timely and controlled manner, in particular for large and complex change programmes, as further elaborated in the Annex.

ICT data integrity risk

The risk that data stored and processed by ICT systems are incomplete, inaccurate or inconsistent across different ICT systems, for example as a result of weak or absent ICT controls during the different phases of the ICT data life cycle (i.e. designing the data architecture, building the data model and/or data dictionaries, verifying data inputs, controlling data extractions, transfers and processing, including rendered data outputs), impairing the ability of an institution to provide services and produce (risk) management and financial information in a correct and timely manner, as further elaborated in the Annex.

ICT outsourcing risk

The risk that engaging a third party, or another Group entity (intra-group outsourcing), to provide ICT systems or related services adversely impacts the institution’s performance and risk management, as further elaborated in the Annex.

3. Implementation

Date of application

9. These Guidelines apply from 1 January 2018.

4. Requirements for the ICT Risk Assessment

Title 1 - General provisions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.1 General principles

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

21.In conducting this assessment, competent authorities should refer to the requirements and standards of good internal governance and risk control arrangements as specified in the EBA Guidelines on Internal Governance (GL 44)[4] and international guidance in this field to the extent these are applicable given the specificity of ICT systems and risks.

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

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

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

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

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

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

2.2 ICT strategy

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

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

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

2.2.1 ICT strategy development and adequacy

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

    a. the senior management[5] of the business line(s) is adequately involved in the definition of the institution's strategic ICT priorities and that, in turn, senior management of the ICT function is aware of the development, design and initiation of major business strategies and initiatives to ensure the continued alignment between ICT systems, ICT services and the ICT function (i.e. those responsible for the management and deployment of these systems and services), and the institution's business strategy, and that ICT are effectively up-dated;

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

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

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

2.2.2 ICT strategy implementation

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

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

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

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

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

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

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

2.3 Overall internal governance

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

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

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

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

2.4 ICT risk in the institution's risk management framework

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

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

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

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

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

2.5 Summary of findings

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

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

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

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

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

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

3.1 General considerations

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

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

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

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

3.2 Identification of material ICT risks

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

3.2.1 Review of the institution's ICT risk profile

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

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

3.2.2 Review of the critical ICT systems and services

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

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

a. they support the core business operations and distribution channels (e.g. ATMs, internet and mobile banking) of the institution;

b. they support essential governance processes and corporate functions, including risk management (e.g. risk management and treasury management systems);

c. they fall under special legal or regulatory requirements (if any) that impose heightened availability, resilience, confidentiality or security requirements (e.g. data protection legislation or possible 'Recovery Time Objectives' (RTO, the maximum time within which a system or process must be restored after an incident) and 'Recovery Point Objective' (RPO, the maximum time period during which data can be lost in case of an incident)) for some systemically important services (if and where applicable));

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

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

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

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

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

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

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

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

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

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

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

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

e. ICT outsourcing risk

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

3.3 Assessment of the controls to mitigate material ICT risks

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

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

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

b. Organisational management and oversight framework;

c. Internal audit coverage and findings; and

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

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

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

3.3.1 ICT risk management policy, processes and tolerance thresholds

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

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

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

c. the institution has implemented a process and underlying procedures for the identification (e.g. 'risk control self-assessments' (RCSA), risk scenario analysis) and monitoring of the involved material ICT risks; and

d. the institution has an ICT risk management reporting in place that provides timely information to senior management and the management body, and which allows senior management and/or the management body to assess and monitor whether the institution´s ICT risk mitigation plans and measures are consistent with the approved risk appetite and/or tolerance thresholds (where relevant) and to monitor changes of material ICT risks.

3.3.2 Organisational management and oversight framework

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

a. clear roles and responsibilities for the identification, assessment, monitoring, mitigation, reporting and oversight of the involved material ICT risk;

b. that the risk responsibilities and roles are clearly communicated, allocated and embedded in all relevant parts (e.g. business lines, IT) and processes of the organisation, including the roles and responsibilities for gathering and aggregating the risk information and reporting it to senior management and/or the management body;

c. that the ICT risk management activities are performed with sufficient and qualitatively appropriate human and technical resources. To assess the credibility of the applicable risk mitigation plans, competent authorities should also assess whether the institution has allocated sufficient financial budgets and/or other required resources for their implementation;

d. an adequate follow-up and response of the management body regarding important findings from the independent control functions regarding the ICT risk(s), taking into account the possible delegation of some aspects to a committee, where this exists; and

e. that exceptions from applicable ICT regulations and policies are recorded and subject to a documented review and reporting by the independent control function with a focus on the related risks.

3.3.3 Internal audit coverage and findings

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

a. the ICT risk control framework is audited with the required quality, depth and frequency and commensurate with the size, activities and the ICT risk profile of the institution;

b. the audit plan includes audits on the critical ICT risks identified by the institution;

c. the important ICT audit findings, including agreed actions, are reported to the management body; and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(b) Controls for managing material ICT security risks

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

a. clearly defined roles and responsibilities regarding:

i. the person(s) and/or committees that are responsible and/or accountable for the day to day ICT security management and the elaboration of the overarching ICT security policies, with attention for their needed independence;
ii. the design, implementation, management and monitoring of ICT security controls;
iii. the protection of critical ICT systems and services by adopting for example a vulnerability assessment process, software patch management, end point protection (e.g. malware virus), Intrusion detection and prevention tools;

iv. the monitoring, classification and handling of external or internal ICT security incidents; including incident response and the resumption and recovery of the ICT systems and services;

v. regular and proactive threat assessments to maintain appropriate security controls.

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

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

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

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

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

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

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

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

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

iii. processes and solutions to secure websites and applications that can be directly attacked from the internet and/or the outside, that can serve as an entry point into the internal ICT systems. In general these include a combination of recognised secure development practices, ICT system hardening and vulnerability scanning practices, and/or the implementation of additional security solutions like for example application firewalls and/or intrusion detection (IDS) and/or intrusion prevention (IPS) systems;

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

(c) Controls for managing material ICT change risks

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

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

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

c. test environments that adequately reflect production environments;

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

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

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

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

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

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

(d) Controls for managing material ICT data integrity risks

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

a. a policy that defines the roles and responsibilities for managing the integrity of the data in the ICT systems (e.g. data architect, data officers[6], data custodians[7], data owners/stewards[8]) and provides guidance on which data are critical from a data integrity perspective and should be subject to specific ICT controls (e.g. automated input validation controls, data transfer controls, reconciliations, etc.) or reviews (e.g. a compatibility check with the data architecture) in the different phases of ICT data life cycle;

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

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

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

[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.

[8] A data steward is responsible for the management and fitness of data elements – both the content and metadata.

58. For supervised institutions that fall under the scope of the BCBS 239 principles for effective risk data aggregation and risk reporting[9], competent authorities should review the institution's risk analysis of its risk reporting and data aggregation capabilities compared to the principles and the prepared documentation thereon, taking into consideration the implementation timeline and transitional arrangements in these principles.

(e) Controls for managing material ICT outsourcing risks

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

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

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

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

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

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

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

3.4 Summary of findings and scoring

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

a. Risk Considerations

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

b. Management and Controls considerations

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

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

Table 1: Supervisory considerations for assigning an ICT risk score

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

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

Annex – ICT Risk Taxonomy

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

ICT risk categories	ICT risks (non exhaustive[10])	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.

[10] 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[10])	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[10])	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[10])	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[10])	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[10])	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.