MFSA MALTA FINANCIAL SERVICES AUTHORITY

BANKING RULE BR/14

OUTSOURCING BY CREDIT INSTITUTIONS AUTHORISED UNDER THE BANKING ACT 1994

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

CONTENTS

INTRODUCTION 1
SCOPE AND APPLICATION 1
DEFINITIONS 2
PART 1 – ASSESSMENT AND NOTIFICATION OF OUTSOURCING ARRANGEMENTS 3
1.1 Assessment of what constitutes outsourcing 3
1.2 Assessment of what constitutes material services or activities 4
1.3 Notification of the intention to outsource a material service or activity 6
PART 2 – GOVERNANCE FRAMEWORK 8
2.1 Sound governance arrangements and third-party risk 8
2.2 Sound governance arrangements and outsourcing 8
2.3 Outsourcing policy 11
2.4 Conflicts of interests 13
2.5 Business continuity plans 13
2.6 Internal audit function 14
2.7 Documentation requirements 14
PART 3 – OUTSOURCING PROCESS 17
3.1 Pre-outsourcing analysis 17
3.2 Supervisory conditions for outsourcing 17
3.3 Risk Assessment of Outsourcing Arrangements 19
3.4 Due Diligence 21
3.5 Contractual Phase 22
3.6 Sub-outsourcing of material services or activities 24
3.7 Security of Data and Systems 25
3.8 Access, Information and Audit Rights 26
3.9 Termination Rights 28
3.10 Oversight of Outsourced Services or Activities 29
3.11 Exit Strategy 30
PART 4 – PROPORTIONALITY: GROUP APPLICATION AND INSTITUTIONAL PROTECTION SCHEMES 32
4.1 Proportionality 32

4.2 OUTSOURCING BY GROUPS AND INSTITUTIONS THAT ARE MEMBERS OF AN INSTITUTIONAL PROTECTION SCHEME 32

REVISIONS LOG

VERSION	DATE ISSUED	DETAILS
1.00	2019	Update of the Rule to align it with amendments to the Banking Act (Chap. 371 of the Laws of Malta).
2.00	2020	Implementation of the EBA Guidelines on Outsourcing Arrangements (EBA/GL/2019/02) and introduction requirements on notification of outsourcing intention.
3.00	2020	Introduction of paragraph 5A regarding the MFSA Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements.
4.00	2022	Amendments to paragraphs 19 and 20 regarding the outsourcing notification time period, and to section 2.3 with respect to the reference to Banking Rule BR/24.
5.00	2022	Addition of paragraph 48A to the Rule to mirror the EBA Guidelines on Outsourcing Arrangements (EBA/GL/2019/02).
6.00	2025	Addition of paragraph 8A clarifying the interaction of specific requirements between the Rule and the DORA Regulation. The deletion of paragraph 5A and of the footnote in paragraph 22 referencing the MFSA Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing arrangements, and the EBA Guidelines on ICT and Security Risk Management (EBA/GL/2019/04).

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

OUTSOURCING BY CREDIT INSTITUTIONS AUTHORISED UNDER THE BANKING ACT 1994

INTRODUCTION

1. In terms of Article 4(7) of the Banking Act 1994 (Chap. 371) ("the Act"), the competent authority ("the Authority") as appointed under Article 3(1) of the Malta Financial Services Act (Chap 330), may make Banking Rules ("the Rules") as may be required for carrying into effect any of the provisions of the Act. The Authority may amend or revoke such Rules. The Rules and any amendment or revocation thereof shall be officially communicated to credit institutions and the Authority shall make copies thereof available to the public.

2. The Rule on the provision of outsourcing by credit institutions is being made pursuant to Article 19A(2) of the Act.

   "The competent authority may issue a Banking Rule laying down the requirements for the information to be submitted regarding the outsourcing service provider and the provision of such outsourced services."

3. It should be emphasised, however, that Rules must not be construed to be solely a substitute for a reading of the Act itself and should be read in conjunction with the Act. The responsibility for observing the law rests entirely with the credit institution and the individual persons concerned.

SCOPE AND APPLICATION

4. The Rule applies to credit institutions, as defined in Article 2(1) of the Act.

5. In drafting this Rule, the Authority has been guided by the Guidelines on Outsourcing Arrangements (EBA/GL/2019/02), issued by the European Banking Authority ('EBA') on the 25 February 2019 (hereinafter referred to for the purposes of this Rule as the 'EBA Guidelines').

6. This Rule specifies the internal governance arrangements, including sound risk management, that credit institutions shall implement when they outsource activities or services, in particular with regard to the outsourcing of material services or activities.

7. Credit institutions as defined in Article 2(1) of the Act shall comply with this Rule on a solo basis, sub-consolidated basis and consolidated basis. The application on a solo basis might be waived by the Authority under Article 21 of Directive 2013/36/EU (the "CRD") or Article 109(1) of the CRD in

conjunction with Article 7 of Regulation (EU) No 575/2013 ("the CRR"). Institutions subject to the CRD shall comply with this Directive and this Rule on a consolidated and sub-consolidated basis as set out in Article 21 and Articles 108 to 110 of the CRD.

8. To this effect, credit institutions shall review and amend accordingly existing outsourcing arrangements with a view to ensuring that these are compliant with this Rule. Where the review of outsourcing arrangements of material services or activities is not finalised by 31 December 2021, credit institutions shall inform the Authority of that fact, including the measures planned to complete the review or the possible exit strategy.

8A. The requirements of this Rule are without prejudice to the requirements of Regulation (EU) 2022/2554 (the "DORA Regulation") insofar as they relate to contractual arrangements on the use of Information and Communication Technology (ICT) services provided by ICT Third Party Providers (TPPs), in line with, and as defined by, the DORA Regulation. In case of any conflict between these outsourcing requirements and the requirements emanating from the DORA Regulation on contractual arrangements on the use of ICT services provided by TPPs, the requirements of the DORA Regulation shall prevail.

DEFINITIONS

9. For the purposes of this Rule, unless the context otherwise requires, the following shall apply:

"*outsourcing*" shall mean an arrangement of any form between a credit institution and a service provider by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the credit institution.

"*material service or activity*" shall mean any service or activity that is considered material as set out in Part 1.2 of this Rule.

"*sub-outsourcing*" shall mean a situation where the service provider under an outsourcing arrangement further transfers an outsourced service or activity to another service provider.

"*service provider*" shall mean a third-party entity that is undertaking an outsourced process, service or activity, or parts thereof, under an outsourcing arrangement.

"*cloud services*" shall mean services provided using cloud computing, that is, a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and

services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

"*public cloud*" shall mean cloud infrastructure available for open use by the general public.

"*private cloud*" shall mean cloud infrastructure available for exclusive use by a single credit institution.

"*community cloud*" shall mean cloud infrastructure available for exclusive use by a specific community of institutions, including several institutions of a single group.

"*hybrid cloud*" shall mean cloud infrastructure that is composed of two or more distinct cloud infrastructures.

Words and expressions used in this Rule which are also used in the Act but which are not defined herein, shall have the same meaning assigned to them as in the Act.

PART 1 – ASSESSMENT AND NOTIFICATION OF OUTSOURCING ARRANGEMENTS

1.1 Assessment of what constitutes outsourcing

10. Where a credit institution intends to outsource a material service or activity, it shall inform the Authority in writing at least 60 days prior to conferring the outsourcing service or activity.

11. Credit institutions shall establish whether an agreement with a third party falls under the definition of outsourcing. Within this assessment, consideration shall be given to:

    i. whether the service or activity (or a part thereof) that is outsourced to a service provider is performed on a recurrent or an ongoing basis by the service provider; and
    ii. whether this service or activity (or part thereof) would normally fall within the scope of service or activity that would or could realistically be performed by credit institutions, even if the credit institution has not performed this service or activity in the past itself.

12. Where an arrangement with a service provider covers multiple services or activities, credit institutions shall consider all aspects of the arrangement within their assessment.

13. As a general principle, credit institutions shall not consider the following as outsourcing:

    a. a service or activity that is legally required to be performed by a service provider, e.g. statutory audit;
    b. market information services (e.g. provision of data by Bloomberg, Moody's, Standard & Poor's, Fitch);
    c. global network infrastructure (e.g. Visa, MasterCard);
    d. clearing and settlement arrangements between clearing houses, central counterparties and settlement institutions and their members;
    e. global financial messaging infrastructures that are subject to oversight by relevant authorities;
    f. correspondent banking services; and
    g. the acquisition of services that would otherwise not be undertaken by the credit institution (e.g. advice from an architect, providing legal opinion and representation in front of the court and administrative bodies, cleaning, gardening and maintenance of the credit institution's premises, medical services, servicing of company cars, catering, vending machine services, clerical services, travel services, post-room services, receptionists, secretaries and switchboard operators), goods (e.g. plastic cards, card readers, office supplies, personal computers, furniture) or utilities (e.g. electivity, gas, water, telephone line).

1.2 Assessment of what constitutes material services or activities

14. Credit institutions shall always consider a service or activity as material in the following situations:

    a. where a defect or failure in its performance would materially impair:
        i. their continuing compliance with the conditions of their authorisation or its other obligations under the CRD, the CRR, Directive 2014/65/EU, Directive (EU) 2015/2366 and Directive 2009/11/EC, and all relevant national legislation, Regulations and Rules transposing the Directives, and their regulatory obligations;
        ii. their financial performance; or
        iii. the soundness or continuity of their banking services and activities;

    b. when operational tasks of internal control functions are outsourced, unless the assessment establishes that a failure to provide the outsourced service or activity or the inappropriate provision of the outsourced service or activity would not have an adverse impact on the effectiveness and quality of the internal control function;

c. when they intend to outsource service or activity of banking activities to an extent that would require authorisation by Authority, as referred to in Part 3.2.

15. Particular attention shall be given to the assessment of the materiality of the activities or services if the outsourcing concerns functions related to core business lines and material services or activities as defined in Regulation 2(1) of the Recovery and Resolution Regulations (S.L. 330.09) and identified by institutions using the criteria set out in Articles 6 and 7 of Commission Delegated Regulation (EU) 2016/778. Activities or services that are necessary to perform functions of core business lines or material services or activities shall be considered as material for the purpose of this Rule, unless the credit institution's assessment establishes that a failure to provide the outsourced service or activity or the inappropriate provision of the outsourced service or activity would not have an adverse impact on the operational continuity of the core business line or material activity.

16. When assessing whether an outsourcing arrangement relates to an activity or service that is material, credit institutions shall take into account, together with the outcome of the risk assessment outlined in Part 3.3, at least the following factors:

a. whether the outsourcing arrangement is directly connected to the provision of banking activities for which they are authorised;
b. the potential impact of any disruption to the outsourced service or activity or failure of the service provider to provide the service at the agreed service levels on a continuous basis on their:
    i. short- and long-term financial resilience and viability, including, if applicable, its assets, capital, costs, funding, liquidity, profits and losses;
    ii. business continuity and operational resilience;
    iii. operational risk, including conduct, information and communication technology (ICT) and legal risks;
    iv. reputational risks;
    v. if applicable, recovery and resolution planning, resolvability and operational continuity in an early intervention, recovery or resolution situation;
c. the potential impact of the outsourcing arrangement on their ability to:
    i. identify, monitor and manage all risks;
    ii. comply with all legal and regulatory requirements;
    iii. conduct appropriate audits regarding the outsourced service or activity;
d. the potential impact on the services provided to its clients;

e. all outsourcing arrangements, the credit institution's aggregated exposure to the same service provider and the potential cumulative impact of outsourcing arrangements in the same business area;
f. the size and complexity of any business area affected;
g. the possibility that the proposed outsourcing arrangement might be scaled up without replacing or revising the underlying agreement;
h. the ability to transfer the proposed outsourcing arrangement to another service provider, if necessary or desirable, both contractually and in practice, including the estimated risks, impediments to business continuity, costs and time frame for doing so ('substitutability');
i. the ability to reintegrate the outsourced service or activity into the credit institution if necessary or desirable;
j. the protection of data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity on the credit institution and its clients, including but not limited to compliance with the CRR.

1.3 Notification of the intention to outsource a material service or activity

17. When informing the Authority of its intention to outsource a material service or activity, the credit institution shall also provide the Authority with the following information:

a. a description of the outsourced service or activity, including the data that are outsourced and whether or not personal data have been transferred or if their processing is outsourced to a service provider;
b. the name of the service provides, the corporate registration number, the legal entity identifier (where available), the registered address and other relevant contact details;
c. the country or countries where the service is to be performed, including the location (i.e. country or regions) of the data;
d. the detailed risk analysis;
e. whether the service provider has a business continuity plan that is suitable for the services provided to the outsourcing institution;
f. in the case of outsourcing to a cloud service provider, the cloud service and deployment models, i.e. public/private/hybrid/community, and the specific nature of the data to be held and the locations (i.e. countries or regions) where such data will be stored;

g. where applicable, the names of any sub-contractors to which important parts of a material service or activity are sub-outsourced, including the country where the sub-contractors are registered, where the services will be performed and, if applicable, the location (i.e. country or region) where the data will be stored;
h. the exit strategy for use if the outsourcing arrangement is terminated by either party or if there is disruption to the provision of the services;
i. an outcome of the assessment of the service provider's substitutability (as easy, difficult or impossible), the possibility of reintegrating a material service or activity into the credit institution or the impact of discontinuing the material services or activities;
j. identification of alternative service providers in line with point (i);
k. information on the resources and measures in place to adequately monitor the outsourced activities; and
l. the estimated annual budget cost.

18. In addition to the information in paragraph 17, the Authority may request the credit institution to provide it with an assurance report regarding the suitability of the outsourcing service provider, which shall include a detailed assessment of the outsourcing arrangement. This report shall be signed by the board of directors of the credit institution. The Authority may also request the credit institution to provide any other information it deems necessary.

19. The Authority shall have sixty days as from the date of notification and submission of the information listed in paragraph 17 by the credit institution or any other information deemed necessary by the Authority, to carry out its assessment on the basis of such information. The Authority may extend this time period where it deems necessary, and it shall inform the credit institution of such extension.

20. The Authority shall, upon completion of its assessment and not later than sixty days, or as extended, where applicable, from the date of notification and submission of the information listed in paragraph 17 or any other information deemed necessary by the Authority, inform the credit institution in writing whether it opposes such intended outsourcing arrangement. Where the Authority opposes the intended outsourcing arrangement, it shall provide the credit institution with the detailed grounds upon which the Authority's decision has been taken.

21. Where the Authority does not inform the credit institution within sixty days, or as extended, where applicable, on whether it opposes the intended outsourcing arrangement in accordance with paragraph 20, such intended

outsourcing arrangement shall be deemed as not opposed. This shall be without prejudice to the credit institution's full responsibility and accountability for complying with its regulatory obligations pursuant to the Act, regulations and Rules issued thereunder, including those related to outsourcing of material services or activities.

PART 2 – GOVERNANCE FRAMEWORK

2.1 Sound governance arrangements and third-party risk

22. As part of the overall internal control framework, including internal control mechanisms, credit institutions shall have a holistic institution-wide risk management framework extending across all business lines and internal units. Under that framework, credit institutions shall identify and manage all their risks, including risks caused by arrangements with third parties. The risk management framework shall also enable credit institutions to make well-informed decisions on risk-taking and ensure that risk management measures are appropriately implemented, including with regard to cyber risks.

23. Credit institutions, taking into account the principle of proportionality in line with Part 4.1, shall identify, assess, monitor and manage all risks resulting from arrangements with third parties to which they are or might be exposed, regardless of whether or not those arrangements are outsourcing arrangements. The risks, in particular the operational risks, of all arrangements with third parties, including the ones referred to in paragraphs 11 and 13, shall be assessed in line with Part 3.3.

24. Credit institutions shall ensure that they comply with all requirements under the CRR, including for their third-party and outsourcing arrangements.

2.2 Sound governance arrangements and outsourcing

25. The outsourcing of services or activities cannot result in the delegation of the board of directors' responsibilities. Credit institutions remain fully responsible and accountable for complying with all of their regulatory obligations, including the ability to oversee the outsourcing of material services or activities.

26. The board of directors is at all times fully responsible and accountable for at least:
    a. ensuring that the credit institution meets on an ongoing basis the conditions with which it must comply to remain

authorised, including any conditions imposed by the Authority;

b. the internal organisation of the credit institution;
c. the identification, assessment and management of conflicts of interest;
d. the setting of the credit institution's strategies and policies (e.g. the business model, the risk appetite, the risk management framework);
e. overseeing the day-to-day management of the credit institution, including the management of all risks associated with outsourcing; and
f. the oversight role of the non-executive directors, including overseeing and monitoring management decision-making.

27. Outsourcing shall not lower the suitability requirements applied to the members sitting on the credit institution's board. Credit institutions shall have adequate competence and sufficient and appropriately skilled resources to ensure appropriate management and oversight of outsourcing arrangements.

28. Credit institutions shall:

a. clearly assign the responsibilities for the documentation, management and control of outsourcing arrangements;
b. allocate sufficient resources to ensure compliance with all legal and regulatory requirements, including this Rule and the documentation and monitoring of all outsourcing arrangements;
c. taking into account Part 4 of this Rule, establish an outsourcing service or activity or designate a senior staff member who is directly accountable to the board of directors (e.g. a key function holder of a control function) and responsible for managing and overseeing the risks of outsourcing arrangements as part of the institution's internal control framework and overseeing the documentation of outsourcing arrangements. Small and less complex credit institutions shall at least ensure a clear division of tasks and responsibilities for the management and control of outsourcing arrangements and may assign the outsourcing service or activity to a member of the credit institution's board of directors.

29. Credit institutions shall maintain at all times sufficient substance and not become 'empty shells' or 'letter-box entities'. To this end, they shall:

a. meet all the conditions of their authorisation at all times, including the board of directors effectively carrying out its responsibilities as set out in paragraph 26 of this Rule;
b. retain a clear and transparent organisational framework and structure that enables them to ensure compliance with legal and regulatory requirements;
c. where operational tasks of internal control functions are outsourced (e.g. in the case of intragroup outsourcing or outsourcing within institutional protection schemes), exercise appropriate oversight and be able to manage the risks that are generated by the outsourcing of material services or activities; and
d. have sufficient resources and capacities to ensure compliance with points (a) to (c).

30. When outsourcing, credit institutions shall at least ensure that:

a. they can take and implement decisions related to their business activities and material services or activities, including with regard to those that have been outsourced;
b. they maintain the orderliness of the conduct of their business and the banking services they provide;
c. the risks related to current and planned outsourcing arrangements are adequately identified, assessed, managed and mitigated, including risks related to ICT and financial technology (fintech);
d. appropriate confidentiality arrangements are in place regarding data and other information;
e. an appropriate flow of relevant information with service providers is maintained;
f. with regard to the outsourcing of material services or activities, they are able to undertake at least one of the following actions, within an appropriate time frame:
    i. transfer the service or activity to alternative service providers;
    ii. reintegrate the service or activity; or
    iii. discontinue the business activities that are depending on the service or activity.
g. where personal data are processed by service providers located in the EU and/or third countries, appropriate measures are implemented and data are processed in accordance with the CRR.

2.3 Outsourcing policy

31. In line with Section 10 of Banking Rule BR/24 on Internal Governance of Credit Institutions Authorised under the Banking Act, the board of directors of a credit institution that has outsourcing arrangements in place or plans on entering into such arrangements shall approve, regularly review and update a written outsourcing policy and ensure its implementation, as applicable, on an individual, sub-consolidated and consolidated basis. Furthermore, in particular, credit institutions shall take into account the requirements set out in Section 22 (on new products and significant changes) of Banking Rule BR/24.

32. The policy shall include the main phases of the life cycle of outsourcing arrangements and define the principles, responsibilities and processes in relation to outsourcing. In particular, the policy shall cover at least:

    a. the responsibilities of the board of directors in line with paragraph 26, including its involvement, as appropriate, in the decision-making on outsourcing of material services or activities;
    b. the involvement of business lines, internal control functions and other individuals in respect of outsourcing arrangements;
    c. the planning of outsourcing arrangements, including:
        i. the definition of business requirements regarding outsourcing arrangements;
        ii. the criteria, including those referred to in Part 1.2, and processes for identifying material services or activities;
        iii. risk identification, assessment and management in accordance with Part 3.3;
        iv. due diligence checks on prospective service providers, including the measures required under Part 3.4;
        v. procedures for the identification, assessment, management and mitigation of potential conflicts of interest, in accordance with Part 2.4;
        vi. business continuity planning in accordance with Part 2.5;
        vii. the approval process of new outsourcing arrangements;
    d. the implementation, monitoring and management of outsourcing arrangements, including:
        i. the ongoing assessment of the service provider's performance in line with Part 3.10;

ii. the procedures for being notified and responding to changes to an outsourcing arrangement or service provider (e.g. to its financial position, organisational or ownership structured, sub-outsourcing);
iii. the independent review and audit of compliance with legal and regulatory requirements and policies;
iv. the renewal processes;

e. the documentation and record-keeping, taking into account the requirements in Part 2.7;
f. the exit strategies and termination processes, including a requirement for a documented exit plan for each material service or activity to be outsourced where such an exit is considered possible taking into account possible service interruptions or the unexpected termination of an outsourcing agreement.

33. The outsourcing policy shall differentiate between the following:

a. outsourcing of material services or activities and other outsourcing arrangements;
b. outsourcing to service providers that are authorised by the Authority and those that are not;
c. intragroup outsourcing arrangements, outsourcing arrangements within the same institutional protection scheme (including entities fully owned individually or collectively by institutions within the institutional protection scheme) and outsourcing to entities outside the group; and
d. outsourcing to service providers located within a Member State and third countries.

34. Credit institutions shall ensure that the policy covers the identification of the following potential effects of material outsourcing arrangements and that these are taken into account in the decision-making process:

a. the credit institution's risk profile;
b. the ability to oversee the service provider and to manage the risks;
c. the business continuity measures; and
d. the performance of their business activities.

34A. The outsourcing policy shall consider the impact of outsourcing on a credit institution's business and the risks it faces (such as operational risks, including legal and IT risks, reputational risks, and concentration risks). The policy shall include the reporting and monitoring arrangements to be implemented from inception to the end of an outsourcing agreement (including drawing up the business case for outsourcing, entering into an outsourcing contract, the implementation of the contract to its expiry,

contingency plans and exit strategies). A credit institution remains fully responsible for all outsourced services and activities and management decisions arising from them. Accordingly, the outsourcing policy shall make it clear that outsourcing does not relieve the credit institution of its regulatory obligations and its responsibilities to its customers.

34B. The policy shall state that outsourcing arrangements shall not hinder effective on-site or off-site supervision of the credit institution and shall not contravene any supervisory restrictions on service and activities. The policy shall also cover intragroup outsourcing (i.e. services provided by a separate legal entity within a credit institution's group) and take into account any specific group circumstances.

34C. The policy shall require that, when selecting material external services providers or when outsourcing activities, the credit institution must take into account whether or not the service provider has in place appropriate ethical standards or a code of conduct.

2.4 Conflicts of interests

35. Credit institutions, in line with Title IV, Section 11, of the EBA Guidelines on internal governance, shall identify, assess and manage conflicts of interests with regard to their outsourcing arrangements.

36. Where outsourcing creates material conflicts of interest, including between entities within the same group or institutional protection scheme, credit institutions need to take appropriate measures to manage those conflicts of interest.

37. When services or activities are provided by a service provider that is part of a group or a member of an institutional protection scheme or that is owned by the credit institution, group or institutions that are members of an institutional protection scheme, the conditions, including financial conditions, for the outsourced service shall be set at arm's length. However, within the pricing of services synergies resulting from providing the same or similar services to several institutions within a group or an institutional protection scheme may be factored in, as long as the service provider remains viable on a stand-alone basis; within a group this shall be irrespective of the failure of any other group entity.

2.5 Business continuity plans

38. Credit institutions, in line with the requirements under Title VI of the EBA Guidelines on internal governance, shall have in place, maintain and periodically test appropriate business continuity plans with regard to

outsourced material services or activities. Credit institutions within a group or institutional protection scheme may rely on centrally established business continuity plans regarding their outsourced service or activity.

39. Business continuity plans shall take into account the possible event that the quality of the provisions of the outsourced material service or activity deteriorates to an unacceptable level or fails. Such plans shall also take into account the potential impact of the insolvency or other failures of service providers and, where relevant, political risks in the service provider's jurisdiction.

2.6 Internal audit function

40. The internal audit function's activities shall cover, following a risk-based approach, the independent review of outsourced activities. The audit plan and programme shall include in particular, the outsourcing arrangements of material services or activities.

41. With regard to the outsourcing process, the internal audit function shall at least ascertain:

    a. that the credit institution's framework for outsourcing, including the outsourcing policy, is correctly and effectively implemented and is in line with the applicable laws and regulation, the risk strategy and the decisions of the board of directors;
    b. the adequacy, quality and effectiveness of the assessment of the materiality of the services or activities;
    c. the adequacy, quality and effectiveness of the risk assessment for outsourcing arrangements and that the risks remain in line with the institution's risk strategy;
    d. the appropriate involvement of governance bodies; and
    e. the appropriate monitoring and management of outsourcing arrangements.

2.7 Documentation requirements

42. As part of their risk management framework, credit institutions shall maintain an updated register of information on all outsourcing arrangements at the credit institution and, where applicable, at sub-consolidated and consolidated levels, as set out in Part 4.2, and shall appropriately document all current outsourcing arrangements, distinguishing between the outsourcing of material services or activities and other outsourcing arrangements. Credit institutions shall maintain the

documentation of ended outsourcing arrangements within the register and the supporting documentation for an appropriate period.

43. Taking into account Part 4 of this Rule, and under the conditions set out in paragraph 103(d), for credit institutions within a group, institutions permanently affiliated to a central body or institutions that are members of the same institutional protection scheme, the register may be kept centrally.

44. The register shall include at least the following information for all existing outsourcing arrangements:

    a. a reference number for each outsourcing arrangements;
    b. the start date and, as applicable, the next contract renewal date, the end date and/or notice periods for the service provider and for the credit institution;
    c. a brief description of the outsourced service or activity, including the data that are outsourced and whether or not personal data (e.g. by providing a yes or no in a separate data field) have been transferred or if their processing is outsourced to a service provider;
    d. a category assigned by the credit institution that reflects the nature of the service or activity as described under point (c) (e.g. information technology (IT), control function), which shall facilitate the identification of different types of arrangements; the name of the service provider, the corporate registration number, the legal entity identifier (where available), the registered address and other relevant contact details, and the name of its parent company (if any);
    e. the country or countries where the service is to be performed, including the location (i.e. country or regions) of the data;
    f. whether or not the outsourced service or activity is considered material, including, where applicable, a brief summary of the reasons why the outsourced service or activity is considered material;
    g. in the case of outsourcing to a cloud service provider, the cloud service and deployment models, i.e. public/private/hybrid/community, and the specific nature of the data to be held and the locations (i.e. countries or regions) where such data will be stored;
    h. the date of the most recent assessment of the materiality the outsourced services or activities.

45. For the outsourcing of material services or activities, the register shall include at least the following additional information:

a. the credit institutions and other firms within the scope of the prudential consolidation or institutional protection scheme, where applicable, that make use of the outsourcing;
b. whether or not the service provider or sub-service provider is part of the group or a member of the institutional protection scheme or is owned by credit institutions within the group or is owned by members of an institutional protection scheme;
c. the date of the most recent risk assessment and a brief summary of the main results;
d. the individual or decision-making body (e.g. the board of directors) in the credit institution that approved the outsourcing arrangement;
e. the governing law of the outsourcing agreement;
f. the dates of the most recent and next scheduled audits, where applicable;
g. where applicable, the names of any sub-contractors to which material parts of a material service or activity are sub-outsourced, including the country where the sub-contractors are registered, where the services will be performed and, if applicable, the location (i.e. country or region) where the data will be stored;
h. an outcome of the assessment of the service provider's substitutability (as easy, difficult or impossible), the possibility of reintegrating a material service or activity into the credit institution or the impact of discontinuing the material service or activity;
i. identification of alternative service providers in line with point (h);
j. whether the outsourced material services or activities supports business operations that are time-critical;
k. the estimated annual budget cost.

46. Credit institutions shall, upon request, make available to the Authority either the full register of all existing outsourcing arrangements or sections specified thereof, such as information on all outsourcing arrangements falling under one of the categories referred to in point (d) of paragraph 44 of this Rule (e.g. all IT outsourcing arrangements). Credit institutions shall provide this information in a processable electronic form (e.g. a commonly used database format, comma separated values).

47. Credit institutions shall, upon request, make available to the Authority all information necessary to enable the Authority to execute the effective supervision of the credit institution, including, where required, a copy of the outsourcing agreement.

48. Credit institutions, without prejudice to Article 19A of the Act, shall adequately inform the Authority in a timely manner or engage in a supervisory dialogue with the Authority about the planned outsourcing of material services or activities and/or where an outsourced service or activity has become material and provide at least the information specified in paragraph 44.

48A. Credit institutions shall inform the Authority in a timely manner of material changes and/or severe events regarding their outsourcing arrangements that could have a material impact on the continuing provision of the credit institutions' business activities.

49. Credit institutions shall appropriately document the assessments made under Part 3 and the results of their ongoing monitoring (e.g. performance of the service provider, compliance with agreed service levels, other contractual and regulatory requirements, updates to the risk assessment).

PART 3 – OUTSOURCING PROCESS

3.1 Pre-outsourcing analysis

50. Before entering into any outsourcing arrangement, credit institutions shall:

a. assess if the outsourcing arrangement concerns a material service or activity, as set out in Part 2;
b. assess if the supervisory conditions for outsourcing set out in Part 3.2 are met;
c. identify and assess all of the relevant risks of the outsourcing arrangement in accordance with Part 2.3;
d. undertake appropriate due diligence on the prospective service provider in accordance with Part 3.4;
e. identify and assess conflicts of interest that the outsourcing may cause in line with Part 2.4.

3.2 Supervisory conditions for outsourcing

51. Credit institutions shall ensure that the outsourcing of banking services or activities to a service provider located in the same or another Member State, where the performance of those services or activities requires authorisation or registration by the Authority, takes place only if one of the following conditions is met:

a. the service provider is authorised or registered by the Authority to perform such banking activities; or
b. the service provider is otherwise allowed to carry out those banking activities in accordance with the relevant national legal framework.

52. Credit institutions shall ensure that the outsourcing of banking services or activities, to an extent that the performance of those services or activities requires authorisation or registration by a competent authority in the Member State where they are authorised, to a service provider located in a third country takes place only if the following conditions are met:

a. the service provider is authorised or registered to provide that banking activity in the third country and is supervised by a relevant competent authority in that third country ("supervisory authority");

b. there is an appropriate cooperation agreement, e.g. in the form of a memorandum of understanding or college agreement, between the competent authorities responsible for the supervision of the service provider; and

c. the cooperation agreement referred to in point (b) shall ensure that the competent authorities are able, at least, to:

i. obtain, upon request, the information necessary to carry out their supervisory tasks pursuant to the CRD, the CRR, Directive (EU) 2015/2366 and Directive 2009/110/EC, and all relevant national legislation, Regulations and Rules transposing the Directives, and their regulatory obligations;
ii. obtain appropriate access to any data, documents, premises or personnel in the third country that are relevant for the performance of their supervisory powers;
iii. receive, as soon as possible, information from the supervisory authority in the third country for investigating apparent breaches of the requirements of the CRD, the CRR, Directive (EU) 2015/2366 and Directive 2009/110/EU, and all relevant national legislation, Regulations and Rules transposing the Directives, and their regulatory obligations; and
iv. cooperate with the relevant supervisory authorities in the third country on enforcement in the case of a breach of the applicable regulatory requirements and national law in the Member State. Cooperation shall include, but not necessarily be limited to, receiving information on potential breaches of the applicable regulatory

requirements from the supervisory authorities in the third country as soon as is practicable.

3.3 Risk Assessment of Outsourcing Arrangements

53. Credit institutions shall assess the potential impact of outsourcing arrangements on their operational risk, shall take into account the assessment results when deciding if the service or activity shall be outsourced to a service provider and shall take appropriate steps to avoid undue additional operational risks before entering into outsourcing arrangements.

54. The assessment shall include, where appropriate, scenarios of possible risk event, including high-severity operational risk events. Within the scenario analysis, credit institutions shall assess the potential impact of failed or inadequate services, including the risks caused by processes, systems, people or external events. Credit institutions, taking into account the principle of proportionality referred to in Part 4.1, shall document the analysis performed and their results and shall estimate the extent to which the outsourcing arrangement would increase or decrease their operational risk. Taking into account Part 4, small and non-complex credit institutions may use qualitative risk assessment approaches, while large or complex credit institutions shall have a more sophisticated approach, including, where available, the use of internal and external loss data to inform the scenario analysis.

55. Within the risk assessment, credit institutions shall also take into account the expected benefits and costs of the proposed outsourcing arrangement, including weighing any risks that may be reduced or better managed against any risks that may arise as a result of the proposed outsourcing arrangement, taking into account at least:

    a. concentration risks, including from:
        i. outsourcing to a dominant service provider that is not easily substitutable; and
        ii. multiple outsourcing arrangements with the same service provider or closely connected service providers;
    b. the aggregated risks resulting from outsourcing several services or activities across the credit institution and, in the case of groups of institutions or institutional protection schemes, the aggregated risks on a consolidated basis or on the basis of the institutional protection scheme;
    c. in the case of significant credit institutions, the step-in risk, i.e. the risk that may result from the need to provide financial

support to a service provider in distress or to take over its business operations; and

d. the measures implemented by the credit institution and by the service provider to manage and mitigate the risks.

56. Where the outsourcing arrangement includes the possibility that the service provider sub-outsources material services or activities to other service providers, credit institutions shall take into account:

a. the risks associated with sub-outsourcing, including the additional risks that may arise if the sub-contractor is located in a third country or a different country from the service provider;

b. the risk that long and complex chains of sub-outsourcing reduce the ability of institutions to oversee the outsourced material service or activity and the ability of the Authority to effectively supervise them.

57. When carrying out the risk assessment prior to outsourcing and during ongoing monitoring of the service provider's performance, credit institutions shall, at least:

a. identify and classify the relevant services or activities and related data and systems as regards their sensitivity and required security measures;

b. conduct a thorough risk-based analysis of the services or activities and related data and systems that are being considered for outsourcing or have been outsourced and address the potential risks, in particular the operational risks, including legal, ICT, compliance and reputational risks, and the oversight limitations related to the countries where the outsourced services are or may be provided and where the data are or are likely to be stored;

c. consider the consequences of where the service provider is located (within or outside the European Union);

d. consider the political stability and security situation of the jurisdictions in question, including:
   i. the laws in force, including laws on data protection;
   ii. the law enforcement provisions in place; and
   iii. the insolvency law provisions that would arise in respect of the urgent recovery of the credit institution's data in particular;

e. define and decide on an appropriate level of protection of data confidentiality, of continuity of the activities outsourced and of the integrity and traceability of data and systems in the context of the

intended outsourcing. Credit institutions shall also consider specific measures, where necessary, for data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with an appropriate key management architecture;

f. consider whether the service provider is a subsidiary or parent undertaking of the credit institution, is included in the scope of accounting consolidation or is a member of or owned by institutions that are members of an institutional protection scheme and, if so, the extent to which the institution controls it or has the ability to influence its actions in line with Part 4.2.

3.4 Due Diligence

58. Before entering into an outsourcing arrangement and considering the operational risks related to the service or activity to be outsourced, credit institutions shall ensure in their selection and assessment process that the service provider is suitable.

59. With regard to material services or activities, credit institutions shall ensure that the service provider has the business reputation, appropriate and sufficient abilities, the expertise, the capacity, the resources (e.g. human, IT, financial), the organisational structure and, if applicable, the required regulatory authorisation(s) or registration(s) to perform the material service or activity in a reliable and professional manner to meet its obligations over the duration of the draft contract.

60. Additional factors to be considered when conducting due diligence on a potential service provider include, but are not limited to:

    a. its business model, nature, scale, complexity, financial situation, ownership and group structure;

    b. the long-term relationships with service providers that have already been assessed and perform services for the credit institution;

    c. whether the service provider is a parent undertaking or subsidiary of the credit institution, is part of the accounting scope of consolidation of the institution or is a member of or is owned by institutions that are members of the same institutional protection scheme to which the institution belongs;

    d. whether or not the service provider is supervised by competent authorities.

61. Where outsourcing involves the processing of personal or confidential data, credit institutions shall be satisfied that the service provider implements appropriate technical and organisational measures to protect the data.

62. Credit institutions shall take appropriate steps to ensure that service providers act in a manner consistent with their values and code of conduct. In particular, with regard to service providers located in third countries and, if applicable, their sub-contractors, credit institutions shall be satisfied that the service provider acts in an ethical and socially responsible manner and adheres to international standards on human rights (e.g. the European Convention on Human Rights), environmental protection and appropriate working conditions, including the prohibition of child labour.

3.5 Contractual Phase

63. The rights and obligations of the credit institution and the service provider shall be clearly allocated and set out in a written agreement.

64. The outsourcing agreement for material services or activities shall set out at least:

    a. clear description of the outsourced service or activity to be provided;

    b. the start and end date, where applicable, of the agreement and the notice periods for the service provider and the credit institution;

    c. the governing law of the agreement;

    d. the parties' financial obligations;

    e. whether the sub-outsourcing of a material service or activity, or material parts thereof, is permitted and, if so, the conditions specified in Part 3.6 that the sub-outsourcing is subject to;

    f. the location(s) (i.e. regions or countries) where the material service or activity will be provided and/or where relevant data will be kept and processes, including the possible storage location, and the conditions to be met, including a requirement to notify the credit institution if the service provider proposes to change the location(s);

g. where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data, as specified in Part 3.7;

h. the right of the credit institution to monitor the service provider's performance on an ongoing basis;

i. the agreed service levels, which shall include precise quantitative and qualitative performance targets for the outsourced service or activity to allow for timely monitoring so that appropriate corrective action can be taken without undue delay if the agreed services levels are not met;

j. the reporting obligations of the service provider to the credit institution, including the communication by the service provider of any development that may have a material impact on the service provider's ability to effectively carry out the material service or activity in line with the agreed service levels and in compliance with applicable laws and regulatory requirements and, as appropriate, the obligations to submit reports of the internal audit function of the service provider;

k. whether the service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;

l. the requirements to implement and test business contingency plans;

m. provisions that ensure that the data that are owned by the credit institution can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the service provider;

n. the obligation of the service provider to cooperate with the Authority and the Resolution Authority of the credit institution, including other persons appointed by them;

o. for institutions, a clear reference to the Resolution Authority's powers, especially to Articles 68 and 71 of the Recovery and Resolution Regulations (S.L. 330.09);

p. the unrestricted right of credit institutions and the Authority to inspect and audit the service provider with regard to, in particular, the material service or activity, as specified in Part 3.8;

q. termination rights, as specified in Part 3.9.

3.6 Sub-outsourcing of material services or activities

65. The outsourcing agreement shall specify whether or not sub-outsourcing of material services or activities, or important parts thereof, is permitted.

66. If sub-outsourcing of material services or activities is permitted, credit institutions shall determine whether the part of the service or activity to be sub-outsourced is, as such, material and, if so, record it in the register.

67. If sub-outsourcing of material services or activities is permitted, the written agreement shall:

a. specify any types of activities that are excluded from sub-outsourcing;
b. specify the conditions to be complied with in the case of sub-outsourcing;
c. specify that the service provider is obliged to oversee those services that it has sub-contracted to ensure that all contractual obligations between the service provider and the credit institution are continuously met;
d. require the service provider to obtain prior specific or general written authorisation from the credit institution before sub-outsourcing data;
e. include an obligation of the service provider to inform the credit institution of any planned sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. This includes planned significant changes of sub-contractors and to the notification period; in particular, the notification period to be set shall allow the outsourcing credit institution at least to carry out a risk assessment of the proposed changes and to object to changes before the planned sub-outsourcing, or material changes thereof, come into effect;
f. ensure, where appropriate, that the credit institution has the right to object to intended sub-outsourcing, or material changes thereof, or that explicit approval is required;
g. ensure that the credit institution has the contractual right to terminate the agreement in the case of undue sub-outsourcing, e.g. where the sub-outsourcing materially increases the risks for the credit institution or where the

service provider sub-outsourced without notifying the credit institution.

68. Credit institutions shall agree to sub-outsourcing only if the sub-contractor undertakes to:
    a. comply with all applicable laws, regulatory requirements and contractual obligations; and
    b. grant the credit institution and the Authority the same contractual rights of access and audit as those granted by the service provider.

69. Credit institutions shall ensure that the service provider appropriately oversees the sub-service providers, in line with the policy defined by the credit institution. If the sub-outsourcing proposed could have material adverse effects on the outsourcing arrangement of a material service or activity or would lead to a material increase of risk, including where the conditions in paragraph 68 would not be met, the credit institution shall exercise its right to object to the sub-outsourcing, if such a right was agreed, and/or terminate the contract.

3.7 Security of Data and Systems

70. Credit institutions shall ensure that service providers, where relevant, comply with appropriate IT security standards.

71. Where relevant (e.g. in the context of cloud or other ICT outsourcing), credit institutions shall define data and system security requirements within the outsourcing agreement and monitor compliance with these requirements on an ongoing basis.

72. In the case of outsourcing to cloud service providers and other outsourcing arrangements that involve the handling or transfer of personal or confidential data, credit institutions shall adopt a risk-based approach to data storage and data processing location(s) (i.e. country or region) and information security considerations.

73. Without prejudice to the requirements under the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), credit institutions, when outsourcing (in particular to third countries), shall take into account differences in national provisions regarding the protection of data. Credit institutions shall ensure that the outsourcing agreement includes the obligation that the service provider protects confidential, personal or otherwise sensitive information and complies with all legal requirements

regarding the protection of data that apply to the credit institution (e.g. the protection of personal data and that banking secrecy or similar legal confidentiality duties with respect to clients' information, where applicable, are observed).

3.8 Access, Information and Audit Rights

74. Credit institutions shall ensure within the written outsourcing arrangement that the internal audit function is able to review the outsourced service or activity using a risk-based approach.

75. Regardless of the materiality of the services or activities, the written outsourcing arrangements between institutions and service providers shall refer to the information gathering and investigatory powers of the Authority and the Resolution Authority under Article 63(1)(a) of the Recovery and Resolution Regulations and Regulation 5 of the Administrative Penalties, Measures and Investigatory Powers Regulations (S.L. 371.05) with regard to service providers located in a Member State and shall also ensure those rights with regard to service providers located in third countries.

76. With regard to the outsourcing of material services or activities, credit institutions shall ensure within the written outsourcing agreement that the service provider grants them and the Authority, including the Resolution Authority, and any other person appointed by them or the Authority, the following:

    a. full access to all relevant business premises (e.g. head offices and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the outsourced service or activity, including related financial information, personnel and the service provider's external auditors ('access and information rights'); and
    b. unrestricted rights of inspection and auditing related to the outsourcing agreement ('audit rights'), to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements.

77. For the outsourcing of services or activities that are not material, credit institutions shall ensure the access and audit rights as set out in paragraph 76(a) and (b) and Part 3.8, on a risk-based approach, considering the nature of the outsourced service or activity and the related operational and reputational risks, its scalability, the potential impact on the continuous performance of its activities and the contractual period. Credit institutions shall take into account that services or activities may become material over time.

78. Credit institutions shall ensure that the outsourcing arrangement or any other contractual arrangement does not impede or limit the effective exercise of the access and audit rights by them, the Authority or third parties appointed by them to exercise these rights.

79. Credit institutions shall exercise their access and audit rights, determine the audit frequency and areas to be audited on a risk-based approach and adhere to relevant, commonly accepted, national and international audit standards.

80. Without prejudice to their final responsibility regarding outsourcing arrangements, credit institutions may use:

    a. pooled audits organised jointly with other clients of the same service provider, and performed by them and these clients or by a third party appointed by them, to use audit resources more efficiently and to decrease the organisational burden on both the clients and the service provider;
    b. third-party certifications and third-party or internal audit reports, made available by the service provider.

81. For the outsourcing of material services or activities, credit institutions shall assess whether third-party certifications and reports as referred to in paragraph 80(b) are adequate and sufficient to comply with their regulatory obligations and shall not rely solely on these reports over time.

82. Credit institutions shall make use of the method referred to in paragraph 80(b) only if they:

    a. are satisfied with the audit plan for the outsourced service or activity;
    b. ensure that the scope of the certification or audit report covers the systems (i.e. processes, applications, infrastructure, data centres, etc.) and key controls identified by the credit institution and the compliance with relevant regulatory requirements;
    c. thoroughly assess the content of the certifications or audit reports on an ongoing basis and verify that the reports or certifications are not obsolete;
    d. ensure that key systems and controls are covered in future versions of the certification of audit report;
    e. are satisfied with the aptitude of the certifying or auditing party (e.g. with regard to rotation of the certifying or auditing company, qualifications, expertise, re-

performance/verification of the evidence in the underlying audit file);

f. are satisfied that the certifications are issued and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place;

g. have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; the number and frequency of such requests for scope modification shall be reasonable and legitimate from a risk management perspective; and

h. retain the contractual right to perform individual audits at their discretion with regard to the outsourcing of material services or activities.

83. In line with the EBA Guidelines on ICT risk assessment under the SREP, institutions shall, where relevant, ensure that they are able to carry out security penetration testing to assess the effectiveness of implemented cyber and internal ICT security measures and processes.

84. Before a planned on-site visit, credit institutions, the Authority and auditors or third parties acting on behalf of the credit institution or the Authority shall provide reasonable notice to the service provider, unless this is not possible due to an emergency or crisis situation or would lead to a situation where the audit would no longer be effective.

85. When performing audits in multi-client environments, care shall be taken to ensure that risks to another client's environment (e.g. impact on service levels, availability of data, confidentiality aspects) are avoided or mitigated.

86. Where the outsourcing arrangement carries a high level of technical complexity, for instance in the case of cloud outsourcing, the credit institution shall verify that whoever is performing the audit – whether it is its internal auditors, the pool of auditors or external auditors acting on its behalf – has appropriate and relevant skills and knowledge to perform relevant audits and/or assessments effectively. The same applies to any staff of the credit institution reviewing third-party certifications or audits carried out by service providers.

3.9 Termination Rights

87. The outsourcing arrangement shall expressly allow the possibility for the credit institution to terminate the arrangement, in accordance with applicable law, including in the following situations:

a. where the provider of the outsourced services or activities is in breach of applicable law, regulations or contractual provisions;
b. where impediments capable of altering the performance of the outsourced services or activities are identified;
c. where there are material changes affecting the outsourcing arrangement or the service provider (e.g. sub-outsourcing or changes of sub-contractors);
d. where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information; and
e. where instructions are given by the credit institution's Authority, e.g. in the case that the Authority is, caused by the outsourcing arrangement, no longer in a position to effectively supervise the credit institution.

88. The outsourcing arrangement shall facilitate the transfer of the outsourced service or activity to another service provider or its re-incorporation into the credit institution. To this end, the written outsourcing arrangement shall:

a. clearly set out the obligations of the existing service provider, in the case of a transfer of the outsourced service or activity to another service provider or back to the credit institution, including the treatment of data;

b. set an appropriate transition period, during which the service provider, after the termination of the outsourcing arrangement, would continue to provide the outsourced service or activities to reduce the risk of disruptions; and

c. include an obligation of the service provider to support the credit institution in the orderly transfer of the service or activity in the event of the termination of the outsourcing agreement.

3.10 Oversight of Outsourced Services or Activities

89. Credit institutions shall monitor, on an ongoing basis, the performance of the service providers with regard to all outsourcing arrangements on a risk-based approach and with the main focus being on the outsourcing of material services or activities, including that the availability, integrity and security of data and information is ensured. Where the risk, nature or scale of an outsourced service or activity has materially changed, credit institutions shall reassess the materiality of that service or activity in line with Part 1.2.

90. Credit institutions shall apply due skill, care and diligence when monitoring and managing outsourcing arrangements.

91. Credit institutions shall regularly update their risk assessment in accordance with Part 3.3 and shall periodically report to the board of directors on the risks identified in respect of the outsourcing of material services or activities.

92. Credit institutions shall monitor and manage their internal concentration risks caused by outsourcing arrangements, taking into account Part 3.3 of this Rule.

93. Credit institutions shall ensure, on an ongoing basis, that outsourcing arrangements, with the main focus being on outsourced material services or activities, meet appropriate performance and quality standards in line with their policies by:

    a. ensuring that they receive appropriate reports from service providers;
    b. evaluating the performance of service providers using tools such as key performance indicators, key control indicators, service delivery reports, self-certification and independent reviews; and
    c. reviewing all other relevant information received from the service provider, including reports on business continuity measures and testing.

94. Credit institutions shall take appropriate measures if they identify shortcomings in the provision of the outsourced service or activity. In particular, credit institutions shall follow up on any indications that service providers may not be carrying out the outsourced material service or activity effectively or in compliance with applicable laws and regulatory requirements. If shortcomings are identified, credit institutions shall take appropriate corrective or remedial actions. Such actions may include terminating the outsourcing agreement, with immediate effect, if necessary.

3.11 Exit Strategy

95. Credit institutions shall have a documented exit strategy when outsourcing material services or activities that is in line with their outsourcing policy and business continuity plans, taking into account at least the possibility of:

    a. the termination of outsourcing arrangements;
    b. the failure of the service provider;
    c. the deterioration of the quality of the service or activity provided and actual or potential business disruptions

caused by the inappropriate or failed provision of the service or activity;

d. material risks arising for the appropriate and continuous application of the service or activity.

96. Credit institutions shall ensure that they are able to exit outsourcing arrangements without undue disruption to their business activities, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of its provision of services to clients. To achieve this, they shall:

a. develop and implement exit plans that are comprehensive, documented and, where appropriate, sufficiently tested (e.g. by carrying out an analysis of the potential costs, impacts, resources and timing implications of transferring an outsourced service to an alternative provider); and
b. identify alternative solutions and develop transition plans to enable the credit institution to remove outsourced services or activities and data from the service provider and transfer them to alternative providers or back to the credit institution or to take other measures that ensure the continuous provision of the material service or activity in a controlled and sufficiently tested manner, taking into account the challenges that may arise because of the location of data and taking the necessary measures to ensure business continuity during the transition phase.

97. When developing exit strategies, credit institutions shall:

a. define the objectives of the exit strategy;
b. perform a business impact analysis that is commensurate with the risk of the outsourced processes, services or activities, with the aim of identifying what human and financial resources would be required to implement the exit plan and how much time it would take;
c. assign roles, responsibilities and sufficient resources to manage exit plans and the transition of activities;
d. define success criteria for the transition of outsourced services or activities and data; and
e. define the indicators to be used for the monitoring of the outsourcing arrangement (as outlined under Part 3.10), including indicators based on unacceptable service levels that should trigger the exit.

PART 4 – PROPORTIONALITY: GROUP APPLICATION AND INSTITUTIONAL PROTECTION SCHEMES

4.1 Proportionality

98. Credit institutions and the Authority shall, when complying with this Rule, have regard to the principle of proportionality. The proportionality principle aims to ensure that governance arrangements, including those related to outsourcing, are consistent with the individual risk profile, the nature and business model of the credit institution and the scale and complexity of their activities so that the objectives of the regulatory requirements are effectively achieved.

99. In applying the requirements in this Rule, credit institutions shall take into account the complexity of the outsourced services or activities, the risks arising from the outsourcing arrangement, the materiality of the outsourced service or activity and the potential impact of the outsourcing on the continuity of their activities.

100. In applying the principle of proportionality, credit institutions and the Authority shall take into account the criteria specified in Title I of the EBA Guidelines on internal governance in line with Article 74(2) of the CRD.

4.2 Outsourcing by groups and institutions that are members of an institutional protection scheme

101. In accordance with Article 109(2) of the CRD, this Rule shall also apply on a sub-consolidated and consolidated basis, taking into account the prudential scope of consolidation. For this purpose, the EU parent undertakings or the parent undertaking in a Member State shall ensure that internal governance arrangements, processes and mechanisms in their subsidiaries are consistent, well integrated and adequate for the effective application of this Rule at all relevant levels.

102. Credit institutions in accordance with paragraph 101, that, as members of the Depositor Compensation Scheme, use centrally provided governance arrangements shall comply with the following:

    a. where those credit institutions have outsourcing arrangements with service providers within the group or the institutional protection scheme, the board of directors of those credit institutions retains, also for these outsourcing arrangements, full responsibility for compliance with all regulatory requirements and the effective application of this Rule;

b. where those credit institutions outsource the operational tasks of internal control functions to a service provider within the group or the institutional protection scheme, for the monitoring and auditing of outsourcing arrangements, institutions shall ensure that, also for these outsourcing arrangements, those operational tasks are effectively performed, including through the receiving of appropriate reports.

103. In addition to paragraph 102, credit institutions within a group for which no waivers have been granted on the basis of Article 109 of the CRD and Article 7 of the CRR, institutions that are a central body or that are permanently affiliated to a central body, or institutions that are members of an institutional protection scheme shall take into account the following:

a. Where the operational monitoring of outsourcing is centralised (e.g. as part of a master agreement for the monitoring of outsourcing arrangements), credit institutions shall ensure that, at least for outsourced material services or activities, both independent monitoring of the service provider and appropriate oversight by each credit institution is possible, including by receiving, at least annually and upon request from the centralised monitoring function a summary of the relevant audit reports for material outsourcing and, upon request, the full audit report;

b. Credit institutions shall ensure that their board of directors will be duly informed of relevant planned changes regarding service providers that are monitored centrally and the potential impact of these changes on the material services or activities provided, including a summary of the risk analysis, including legal risks, compliance with regulatory requirements and the impact on service levels, in order for them to assess the impact of these changes;

c. Where those credit institutions within the group, institutions affiliated to a central body or institutions that are part of an institutional protection scheme rely on a central pre-outsourcing assessment of outsourcing arrangements, as referred to in Part 3.1, each credit institution shall receive a summary of the assessment and ensure that it takes into consideration its specific structure and risks within the decision-making process;

d. Where the register of all existing outsourcing arrangements, as referred to in Part 2.7, is established and maintained centrally within a group or institutional protection scheme,

the Authority, all credit institutions shall be able to obtain their individual register without undue delay. This register shall include all outsourcing arrangements, including outsourcing arrangements with service providers inside that group or institutional protection scheme;

e. Where those credit institutions rely on an exit plan for a material service or activity that has been established at group level, within the institutional protection scheme or by the central body, all credit institutions shall receive a summary of the plan and be satisfied that the plan can be effectively executed.

104. Where waivers have been granted pursuant to Article 21 of the CRD or Article 109(1) of the CRD in conjunction with Article 7 of the CRR, the provisions of this Rule shall be applied by the parent undertaking in a Member State for itself and its subsidiaries or by the central body and its affiliates as a whole.

105. Credit institutions that are subsidiaries of an EU parent undertaking or of a parent undertaking in a Member State to which no waivers have been granted on the basis of Article 21 of the CRD or Article 109(1) of the CRD in conjunction with Article 7 of the CRR shall ensure that they comply with this Rule on an individual basis.

Malta Financial Services Authority

Triq L-Imdina, Zone 1

Central Business District, Birkirkara, CBD 1010, Malta

communications@mfsa.mt

www.mfsa.mt