MFSA MALTA FINANCIAL SERVICES AUTHORITY

BANKING RULE BR/24

INTERNAL GOVERNANCE OF CREDIT INSTITUTIONS LICENSED UNDER THE BANKING ACT

CONTENTS

REVISIONS LOG

VERSION	DATE ISSUED	DETAILS
1.00	2022	Transposition of certain provisions of the CRD and implementation of the EBA Guidelines on internal governance (EBA/GL/2017/11), as amended by the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05).
2.00	June 2022	Amendment to include reference to EBA Guidelines on ICT and Security Risk Management (EBA/GL/2019/04) issued on the 29th November 2019 and new paragraph 299 for clarity purposes.
3.00	October 2024	Amendments in Section 1 of Part 2 of the Rule to implement the EBA Guidelines on benchmarking of diversity practices, including diversity policies and gender pay gap, under Directive 2013/36/EU and Directive (EU) 2019/2034 (EBA/GL/2023/08) issued on the 18th December 2023.
4.00	December 2024	Amendments to paragraphs 73, 283 and 299 to align with changes brought by the implementation of EU Regulation No. 2022/2554 on digital operational resilience for the financial sector and Amending EU Directive No. 2022/2556. See Transposition of Directive (EU) 2022/2556 on Digital Operational Resilience for the Financial Sector – Amendments to the Authority's Rules.
5.00	May 2025	Amendments to paragraphs 4(c), 73(a), and 299 to include reference to EBA Guidelines EBA/GL/2025/02 amending Guidelines EBA/GL/2019/04 on ICT and Security Risk Management.
6.00	February 2026	Introduction of a new Section 6 under Part 2 entitled "Regulatory Approval for Individuals assuming Key Positions" specifying the process, criteria, and obligations of institutions under such circumstances.

INTERNAL GOVERNANCE BY CREDIT INSTITUTIONS LICENSED UNDER THE BANKING ACT 1994

INTRODUCTION

1. In terms of Article 4(6) of the Banking Act 1994 ("the Act"), the competent authority ("the Authority") as appointed under Article 3(1) of the Malta Financial Services Authority Act (Chap. 330), may issue Banking Rules ("the Rules") as may be required for the carrying into effect of any 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 Internal Governance by credit institutions is being made pursuant to Article 17B (1) of the Act:

   "*Every credit institution shall put in place robust governance arrangements which include a clear organisational structure with well defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks it is or might be exposed to, adequate internal control mechanisms including sound administrative and accounting procedures, and remuneration policies and practices that are consistent with and promote sound and effective risk management*:

   Provided that such remuneration policies and practices shall be gender neutral.".

SCOPE AND APPLICATION

3. The Rule applies to all credit institutions licensed under the Act and credit institutions shall ensure compliance with the provisions of this Rule.

4. The scope of this Rule is to:

   a. transpose Articles 77(1) and (3), 78(1) and (6), 80-87, 88(1), and 91(9)-(12) of the CRD; and
   b. implement the EBA Guidelines on internal governance under Directive 2013/36/EU issued on 2 July 2021 (EBA/GL/2021/05);
   c. implement the EBA Guidelines EBA/GL/2025/02 amending Guidelines EBA/GL/2019/04 on ICT and Security Risk Management issued on 11 February 2025.

d. implement the EBA Guidelines on benchmarking of diversity practices, including diversity policies and gender pay gap, under Directive 2013/36/EU and Directive (EU) 2019/2034 (EBA/GL/2023/08).

5. This Rule specifies internal governance arrangements, processes and mechanisms that credit institutions shall implement in accordance with article 17B(1) of the Banking Act to ensure effective and prudent management of credit institutions.

6. Credit institutions shall comply with this Rule on an individual, sub-consolidated and consolidated basis, in accordance with the level of application set out in paragraph 9 of Banking Rule BR/12.

7. This Rule shall not substitute any other law, unless otherwise specified, by which credit institutions subject to this Rule shall abide more specifically with the applicable provisions in the Act, any other European and national legislation and the Regulations. Particularly, the relevant provisions of the Act and the Banking Act (Supervisory Review) Regulations (S.L. 371.16) shall apply to credit institutions.

DEFINITIONS

8. For the purpose of this Rule, the following definitions shall apply:

"chief executive officer (CEO)" means the person who is responsible for managing and steering the overall business activities of a credit institution;

"chief financial officer (CFO)" means the person who is overall responsible for managing all of the following activities: financial resources management, financial planning and financial reporting;

"consolidating credit institution" means a credit institution that is required to abide by the prudential requirements on the basis of the consolidated situation in accordance with Part 1, Title 2, Chapter 2 of the CRR;

"directorship" means a position as a director sitting on the board of directors of a credit institution or another legal entity;

"heads of internal control functions" means the persons at the highest hierarchical level in charge of effectively managing the day-to-day operation of the independent risk management, compliance and internal audit functions;

"key function holders" means persons who have significant influence over the direction of the credit institution but who are not directors sitting on the board and are not the CEO. They include the heads of internal control functions and the CFO, where they are not directors sitting on the board, and, where identified on a risk-based approach by credit institutions, other key function holders.

Other key function holders might include heads of significant business lines, European Economic Area/European Free Trade Association branches, third country subsidiaries and other internal functions;

"listed CRD-credit institution" means credit institutions whose financial instruments are admitted to trading on a regulated market or on a multilateral trading facility as defined under Article 2(1) of the Financial Markets Act (Chapter 345 of the Laws of Malta), in one or more Member States;

"prudential consolidation" means the application of the prudential rules set out in the CRD as transposed in the Act, any Regulations and Rules issued thereunder and in any binding legal instruments issued under the CRD, and the CRR on a consolidated or sub-consolidated basis, in accordance with Part 1, Title 2, Chapter 2 of the CRR;

"risk appetite" means the aggregate level and types of risk a credit institution is willing to assume within its risk capacity, in line with its business model, to achieve its strategic objectives;

"risk capacity" means the maximum level of risk a credit institution is able to assume given its capital base, its risk management and control capabilities, and its regulatory constraints;

"risk culture" means a credit institution's norms, attitudes and behaviours related to risk awareness, risk-taking and risk management, and the controls that shape decisions on risks. Risk culture influences the decisions of management and employees during the day-to-day activities and has an impact on the risks they assume;

"shareholder" means a person who owns shares in a credit institution or, depending on the legal form of a credit institution, other owners or members of the credit institution;

"significant credit institutions" means credit institutions referred to in Article 131 of the CRD (global systemically important credit institutions (G-SIIs) and other systemically important credit institutions (O-SIIs)), and, as appropriate, other credit institutions determined by the Authority or national law, based on an assessment of the credit institution's size and internal organisation, and the nature, scope and complexity of their activities;

"staff" means all employees of a credit institution and its subsidiaries within its scope of consolidation, including subsidiaries not subject to the CRD as transposed in the Act, any Regulations and Rules issued thereunder, and all directors sitting on the board.

9. For the purposes of applying the requirements and supervisory powers laid down in the Act and any regulations and Banking Rules made or issued thereunder transposing the CRD, in any binding legal instruments issued under

the CRD or in the CRR, on a consolidated or sub-consolidated basis in accordance with this Act and any regulations made or issued thereunder transposing the CRD, with any binding legal instruments issued under the CRD and with the CRR, the terms “institution” and “parent undertaking" used in this Rule shall also include, where applicable:

(a) financial holding companies and mixed financial holding companies that have been granted approval in accordance with article 11B of the Act and, or Article 21a of the CRD;

(b) designated institutions controlled by an EU parent financial holding company, an EU parent mixed financial holding company, a parent financial holding company in a Member State or a parent mixed financial holding company in a Member State where the relevant parent is exempted in accordance with article 11B(5) of the Act and, or Article 21a(4) of the CRD; and

(c) financial holding companies, mixed financial holding companies or institutions designated pursuant to article 29AA(1)(f) of the Act and, or Article 21a(6)(d) of the CRD.

10. For the purposes of applying the requirements and supervisory powers laid down in Sections 5.4, 27, 28, 30, 33-35 and 37 and paragraphs 14, 80, 265-269, 273 and 284-294 of this Rule on a consolidated or sub-consolidated basis in accordance with this Act and any regulations and Banking Rules made or issued thereunder transposing the CRD, with any binding legal instruments issued under the CRD and with the CRR, the term "credit institution" shall also include:

(a) financial holding companies and mixed financial holding companies that have been granted approval in accordance with article 11B of the Act and, or Article 21a of the CRD;

(b) designated institutions controlled by an EU parent financial holding company, an EU parent mixed financial holding company, a parent financial holding company in a Member State or a parent mixed financial holding company in a Member State where the relevant parent is exempted in accordance with article 11B(5) of the Act and, or Article 21a(4) of the CRD; and

(c) financial holding companies, mixed financial holding companies or institutions designated pursuant to article 29AA(1)(f) of the Act and, or Article 21a(6)(d) of the CRD.

PART 1 – PROPORTIONALITY

11. The proportionality principle encoded in Article 17B(2) of the Act aims to ensure that internal governance arrangements are consistent with the individual risk profile and business model of the credit institution, so that the objectives of the regulatory requirements and provisions are effectively achieved.

12. Credit institutions shall take into account their size and internal organisation, and the nature, scale and complexity of their activities, when developing and implementing internal governance arrangements. Significant credit institutions shall have more sophisticated governance arrangements, while small and less complex credit institutions may implement simpler governance arrangements. Credit institutions shall however note that the size or systemic importance of a credit institution may not, by itself, be indicative of the extent to which an institution is exposed to risks.

13. For the purpose of the application of the principle of proportionality and in order to ensure an appropriate implementation of the regulatory requirements and this Rule, credit institutions shall take into account the following criteria:

    a. the size in terms of the balance-sheet total of the credit institution and its subsidiaries within the scope of prudential consolidation;

    b. the geographical presence of the credit institution and the size of its operations in each jurisdiction;

    c. the legal form of the credit institution, including whether the credit institution is part of a group and, if so, the proportionality assessment for the group;

    d. whether the credit institution is listed or not;

    e. whether the credit institution is authorised to use internal models for the measurement of capital requirements (e.g. the Internal Ratings Based Approach);

    f. the type of authorised activities and services performed by the credit institution (e.g. see also in the First Schedule to the Act and Annex 1 to Directive 2014/65/EU);

    g. the underlying business model and strategy; the nature and complexity of the business activities, and the credit institution's organisational structure;

    h. the risk strategy, risk appetite and actual risk profile of the credit institution, taking into account also the result of the SREP capital and SREP liquidity assessments;

i. the ownership and funding structure of the credit institution;

j. the type of clients (e.g. retail, corporate, institutional, small businesses, public entities) and the complexity of the products or contracts;

k. the outsourced activities and distribution channels;

l. the existing information technology (IT) systems, including continuity systems and outsourcing activities in this area; and

m. whether the credit institution falls under the definition in Points 145 and 146 of Article 4(1) of the CRR of a small and non-complex institution or a large institution.

PART 2 – ROLE AND COMPOSITION OF THE BOARD OF DIRECTORS AND COMMITTEES

Section 1: Board of Directors

14. The board of directors shall define, oversee and be accountable for the implementation of the governance arrangements that ensure effective and prudent management of a credit institution, including the segregation of duties in the organisation and the prevention of conflicts of interest.

Those arrangements shall comply with the following principles:

(a) the board of directors must have the overall responsibility for the credit institution and approve and oversee the implementation of the credit institution's strategic objectives, risk strategy and internal governance;

(b) the board of directors must ensure the integrity of the accounting and financial reporting systems, including financial and operational controls and compliance with the law and relevant standards;

(c) the board of directors must oversee the process of disclosure and communications;

(d) the board of directors must be responsible for providing effective oversight of senior management;

(e) the chairperson of the board of directors of a credit institution must not exercise simultaneously the functions of a chief executive officer within the same credit institution, unless justified by the credit institution and authorised by the authority.

The board of directors shall monitor and periodically assess the effectiveness of the credit institution's governance arrangements and shall take appropriate steps to address any deficiencies.

15. With respect to requirements related to the Board of Directors, the requirements laid out in Article 14(2) to (6) of the Act shall apply to credit institutions.

16. In addition to the Act's requirements, credit institutions shall devote adequate human and financial resources to the induction and training of directors.

17. Credit institutions and their respective nomination committees established according to this Rule shall engage in a broad set of qualities and competences when recruiting directors and for that purpose shall put in place a policy promoting diversity on the board of directors.

18. Pursuant to regulation 16 of the Banking Act (Supervisory Review) Regulations (371.16), the Authority shall collect the information disclosed in accordance with Article 435(2)(c) of the CRR and shall use it to benchmark diversity practices. The Authority shall provide the EBA with that information. For the purpose of submitting that information to the Authority, credit institutions shall comply with the EBA Guidelines on benchmarking of diversity practices, including diversity policies and gender pay gap, under Directive 2013/36/EU and Directive (EU) 2019/2034 (EBA/GL/2023/08), including the reporting requirements specified in the templates as found in the Annexes (I – XI) to the EBA Guideline.

The aforementioned EBA Guidelines specify the information to be provided by institutions regarding the composition of the management body, diversity policies and the gender pay gap at the level of the management body. In this regard, institutions shall refer and adhere to the EBA Guidelines in their entirety, and to any amendments carried out to such Guidelines from time to time, including details about the reporting requirements and specifications regarding the governance system to be provided, the data on members of management body, and the calculation of the gender pay gap.

The Authority shall communicate directly with the credit institutions which fall within the scope of this data collection exercise. Institutions that form part of the sample shall be informed at least 3 months before the submission of data is requested.

In-scope institutions shall submit to the Authority the data as specified in the aforementioned Annexes on an individual basis, in the data exchange formats and representations as specified by the Authority.

For the purpose of the first exercise, in-scope institutions shall submit the requested data to the Authority by 30 April 2025 with reference date 31 December 2024. The exercise shall subsequently be carried out every 3 years with the end of the calendar year as reference date (31 December) and shall be submitted to the Authority by 30 April of that same year.

By way of derogation from the fifth subparagraph of this paragraph, financial information shall be submitted using the latest available accounting year-end figures, where this deviates from the calendar year-end.

Prior to submitting the information to the Authority, credit institutions shall undertake rigorous checks and controls to ensure completeness, plausibility and accuracy of the data and apply necessary corrections.

Following the submission of data, the Authority may request in-scope institutions clarifications on and/or resubmissions of the data, in cases of data quality issues within the reporting and if and when it deems so appropriate. Any corrections to the data shall be submitted to the Authority without undue delay.

19. The duties of the board of directors shall be clearly defined, distinguishing between the duties of the executive directors and of the non-executive directors. The responsibilities and duties of the board of directors shall be described in a written document and duly approved by the board of directors.

20. All directors sitting on the board shall be fully aware of the structure and responsibilities of the board of directors, and of the division of tasks between different functions of the board of directors and its committees. In order to have appropriate checks and balances in place, its decision-making shall not be dominated by a single member or a small subset of its members. Non-executive and executive directors shall interact effectively and provide each other with sufficient information to allow them to perform their respective roles. In order to have appropriate checks and balances in place, the decision-making within the board of directors shall not be dominated by a single director or a small subset of its directors.

21. The board of directors' responsibilities shall, *inter alia*, include setting, approving and overseeing the implementation of:

    a. the overall business strategy and the key policies of the credit institution within the applicable legal and regulatory framework, taking into account the credit institution's long term financial interests and solvency;

    b. the overall risk strategy, including the credit institution's risk appetite and its risk management framework and measures to ensure that the board of directors devotes sufficient time to risk issues;

c. an adequate and effective internal governance and internal control framework that:

    i. includes a clear organisational structure and well-functioning independent internal risk management, compliance and audit functions that have sufficient authority, stature and resources to perform their functions;
    ii. ensures compliance with applicable regulatory requirements in the context of the prevention of money laundering and terrorism financing;

d. the amounts, types and distribution of both internal capital and regulatory capital to adequately cover the risks of the credit institution;

e. targets for the liquidity management of the credit institution;

f. a remuneration policy that is in line with the remuneration principles set out in Banking Rule BR/21, especially those set out in paragraphs 16-22;

g. arrangements aimed at ensuring that the individual and collective suitability assessments of the board of directors are carried out effectively, that the composition and succession planning of the board of directors are appropriate, and that the board of directors performs its functions effectively;

h. a selection and suitability assessment process for key function holders;

i. arrangements aimed at ensuring the internal functioning of each committee of the board of directors, when established, detailing the:
    i. role, composition and tasks of each of them;
    ii. appropriate information flow, including the documentation of recommendations and conclusions, and reporting lines between each committee and the board of directors, the Authority and other parties;

j. a risk culture in line with Section 12 of this Rule, which addresses the credit institution’s risk awareness and risk-taking behaviour;

k. a corporate culture and values in line with Section 13 of this Rule, which fosters responsible and ethical behaviour, including a code of conduct or similar instrument;

l. a conflict of interest policy at institutional level in line with Section 14 of this Rule and for staff in line with Section 15 of this Rule; and

m. arrangements aimed at ensuring the integrity of the accounting and financial reporting systems, including financial and operational controls and compliance with the law and relevant standards.

22. When setting, approving and overseeing the implementation of the aspects listed above, the board of directors shall aim at ensuring a business model, governance arrangements, including a risk management framework that take into account all risks. When taking into account all risks credit institutions are exposed to, credit institutions shall take into account all relevant risk factors, including environmental, social and governance risk factors. Credit institutions shall consider that the latter may drive their prudential risks, including credit risks, e.g. via risk factors related to the transition to a sustainable economy or external physical climate-related events that may affect debtors, market, liquidity, operational risks and also reputational risks, e.g. via social and governance risk factors, e.g. in the context of outsourcing arrangements. Such risks include, e.g. legal risks in the area of contractual or labour law, risks related to potential human rights violations or other ESG risk factors that may affect the country where a service provider is located and its ability to provide the agreed service levels.

23. The board of directors shall oversee the process of disclosure and communications with external stakeholders and the Authority.

24. All directors sitting on the board shall ensure that they are informed about the overall activity, financial and risk situation of the credit institution, taking into account the economic environment, and about decisions taken that have a major impact on the credit institution's business.

    A director sitting on the board may be responsible for an internal control function as referred to in Section 24.1 of this Rule, however, the director shall not have other mandates that would compromise the director's internal control activities and the independence of the internal control function.

25. The board of directors shall monitor, periodically review and address any weaknesses identified regarding the implementation of processes, strategies and policies related to the responsibilities listed in paragraphs 21 and 22. The internal governance framework and its implementation shall be reviewed and updated on a periodic basis taking into account the proportionality principle, as further explained in Part 1 of this Rule. A deeper review shall be carried out where material changes affect the credit institution.

Section 2: Executive Directors Sitting on the Board

26. The executive directors sitting on the board shall engage actively in the business of a credit institution and shall take decisions on a sound and well-informed basis.

27. The executive directors sitting on the board shall be responsible for the implementation of the strategies set by the board of directors and discuss regularly the implementation and appropriateness of those strategies with the

non-executive directors sitting on the board. The operational implementation may be performed by the credit institution's management.

28. The executive directors sitting on the board shall constructively challenge and critically review propositions, explanations and information received when exercising its judgement and taking decisions. The executive directors sitting on the board shall comprehensively report, and inform regularly and where necessary without undue delay the non-executive directors sitting on the board of the relevant elements for the assessment of a situation, the risks and developments affecting or that may affect the credit institution, e.g. material decisions on business activities and risks taken, the evaluation of the credit institution's economic and business environment, liquidity and sound capital base, and assessment of its material risk exposures.

29. Without prejudice to Directive 2015/849/EU of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (the Anti-Money Laundering Directive or the AMLD), as transposed in national legislation, the board of directors shall identify one of its directors with the requirements under Article 46(4) of the AMLD who is responsible for the implementation of the laws, regulations and administrative provisions necessary to comply with this directive, including the corresponding AML/CFT policies and procedures in the credit institution and at the level of the board of directors. The board of directors as a collegial body remains responsible as a whole.

Section 3: Non-Executive Directors Sitting on the Board

30. The role of the non-executive directors sitting on the board shall include monitoring and constructively challenging the strategy of the credit institution.

31. Without prejudice to the Act, the non-executive directors sitting on the board shall include independent members.

32. Without prejudice to the responsibilities assigned under the Companies Act (Cap. 386 of the Laws of Malta), the non-executive directors sitting on the board shall:

    (a) oversee and monitor management decision-making and actions and provide effective oversight of the executive directors sitting on the board, including monitoring and scrutinising its individual and collective performance and the implementation of the credit institution's strategy and objectives;

    (b) constructively challenge and critically review proposals and information provided by executive directors sitting on the board, as well as its decisions;

(c) taking into account the proportionality principle as set out in Title 1 of this Rule, appropriately fulfil the duties and role of the risk committee, the remuneration committee and the nomination committee, where no such committees have been set up;

(d) ensure and periodically assess the effectiveness of the credit institution's internal governance framework and take appropriate steps to address any identified deficiencies;

(e) oversee and monitor that the credit institution's strategic objectives, organisational structure and risk strategy, including its risk appetite and risk management framework, as well as other policies (e.g. remuneration policy) and the disclosure framework are implemented consistently;

(f) monitor that the risk culture of the credit institution is implemented consistently;

(g) oversee the implementation and maintenance of a code of conduct or similar and effective policies to identify, manage and mitigate actual and potential conflicts of interest;

(h) oversee the integrity of financial information and reporting, and the internal control framework, including an effective and sound risk management framework;

(i) ensure that the heads of internal control functions are able to act independently and, regardless the responsibility to report to other internal bodies, business lines or units, can raise concerns and warn the non-executive directors sitting on the board directly, where necessary, when adverse risk developments affect or may affect the credit institution; and

(j) monitor the implementation of the internal audit plan, after the prior involvement of the risk and audit committees, where such committees are established.

Section 4: Role of the Chairperson of the Board of Directors

33. The chairperson of the board of directors shall lead the board of directors, shall contribute to an efficient flow of information within the board of directors and between the board of directors and the committees thereof, where established, and shall be responsible for its effective overall functioning.

34. The chairperson shall encourage and promote open and critical discussion and ensure that dissenting views can be expressed and discussed within the decision-making process.

As a general principle, the chairperson of the board of directors shall be a non-executive member. Where the chair is permitted to assume executive duties, the credit institution shall have measures in place to mitigate any adverse impact on the credit institution's checks and balances (e.g. by designating a lead board member or a senior independent board member, or by having a larger number of non-executive members within the board of directors). In particular, in accordance with paragraph 14(e) of this Rule, the chairperson of the board of directors shall not exercise simultaneously the functions of a CEO within the same credit institution, unless justified by the credit institution and authorised by the Authority.

35. The chairperson shall set meeting agendas and ensure that strategic issues are discussed with priority. The chairperson shall ensure that decisions of the board of directors are taken on a sound and well-informed basis and that documents and information are received in enough time before the meeting.

36. The chairperson of the board of directors shall contribute to a clear allocation of duties between directors of the board and the existence of an efficient flow of information between them, in order to allow the non-executive directors sitting on the board to constructively contribute to discussions and to cast their votes on a sound and well-informed basis.

Section 5: Committees

5.1 Setting up Committees

37. All credit institutions that are themselves significant, considering the individual, sub-consolidated and consolidated levels, shall establish risk, nomination and remuneration committees to advise the non-executive directors sitting on the board and to prepare the decisions to be taken by the non-executive directors sitting on the board.

38. Less significant credit institutions, including when they are within the scope of prudential consolidation of a credit institution that is significant in a sub-consolidated or consolidated situation, are not obliged to establish those committees. Less significant credit institutions shall take into account their size and internal organisation, and the nature, scale and complexity of their activities when deciding whether to establish such committees.

39. Where no risk or nomination committee is established, the references in this Rule to those committees shall be construed as applying to the non-executive directors sitting on the board, taking into account the principle of proportionality as set out in Title 1 of this Rule.

40. Credit institutions may, taking into account the criteria set out in Title 1 of this Rule, establish other committees (e.g. anti-money laundering/counter terrorist financing (AML/CFT), ethics, conduct and compliance committees).

41. Credit institutions shall ensure a clear allocation and distribution of duties and tasks between specialised committees of the board of directors.

42. Each committee shall have a documented mandate, including the scope of its responsibilities, from the non-executive directors sitting on the board and establish appropriate working procedures.

43. Committees shall support the non-executive directors sitting on the board in specific areas and facilitate the development and implementation of a sound internal governance framework. Delegating to committees does not in any way release the non-executive directors sitting on the board from collectively fulfilling their duties and responsibilities.

5.2 Composition of Committees

44. All committees shall be chaired by a non-executive director sitting on the board who is able to exercise objective judgement.

45. Independent non-executive directors sitting on the board shall be actively involved in committees.

46. Where committees have to be set up in accordance with the CRD, as transposed in the Act, regulations made and Rules issued thereunder, or with national law, they shall be composed of at least three members.

47. Credit institutions shall ensure, taking into account the size of the board of directors and the number of independent non-executive directors sitting on the board, that committees are not composed of the same group of members that forms another committee.

48. Credit institutions shall occasionally rotate chairs and members of committees, taking into account the specific experience, knowledge and skills that are individually or collectively required for those committees.

49. The following committees shall be composed as follows:

    a. the audit committee shall be composed in accordance with Section 5.5 of this Rule;
    b. the remuneration committee shall be composed in accordance with paragraphs 70 and 71 of BR/21.

50. The risk and nomination committees shall be composed of non-executive directors of the board.

51. In G-SIIs and O-SIIs, the nomination committee shall include a majority of members who are independent and chaired by an independent member. In other significant credit institutions, determined by the Authority or Maltese law, the nomination committee shall include a sufficient number of members

who are independent. Such credit institutions may also consider as a good practice having a chair of the nomination committee who is independent.

52. Members of the nomination committee shall have, individually and collectively, appropriate knowledge, skills and expertise concerning the selection process and suitability requirements.

53. In G-SIIs and O-SIIs, the risk committee shall include a majority of members who are independent. In G-SIIs and O-SIIs the chairperson of the risk committee shall be an independent member. In other significant credit institutions, determined by the Authority or national law, the risk committee shall include a sufficient number of members who are independent and the risk committee shall be chaired, where possible, by an independent member. In all credit institutions, the chairperson of the risk committee shall be neither the chair of the board of directors nor the chair of any other committee.

54. Members of the risk committee shall have, individually and collectively, appropriate knowledge, skills and expertise concerning risk management and control practices.

5.3 Committees' Processes

55. Committees shall regularly report to non-executive directors sitting on the board.

56. Committees shall interact with each other as appropriate. Without prejudice to paragraph 47, such interaction could take the form of cross-participation so that the chairperson or a member of a committee may also be a member of another committee.

57. Members of committees shall engage in open and critical discussions, during which dissenting views are discussed in a constructive manner.

58. Committees shall document the agendas of committee meetings and their main results and conclusions.

59. The risk and nomination committees shall at least:

    a. have access to all relevant information and data necessary to perform their role, including information and data from relevant corporate and control functions (e.g. legal, finance, human resources, IT, internal audit, risk, compliance, including information on AML/CFT compliance and aggregated information on suspicious transaction reports, and ML/TF risk factors);

    b. receive regular reports, ad hoc information, communications and opinions from heads of internal control functions concerning the current risk profile of the credit institution, its risk culture and its risk limits, as

well as on any material breaches that may have occurred, with detailed information on and recommendations for corrective measures taken, to be taken or suggested to address them;

c. periodically review and decide on the content, format and frequency of the information on risk to be reported to them; and

d. where necessary, ensure the proper involvement of the internal control function and other relevant functions (human resources, legal, finance) within their respective areas of expertise and/or seek external expert advice.

5.4 Risk Committee

60. The board of directors of a credit institution shall approve and periodically review the strategies and policies for taking up, managing, monitoring and mitigating the risks that the credit institution is or might be exposed to, including those posed by the macroeconomic environment in which it operates in relation to the status of the business cycle.

61. The board of directors of a credit institution shall devote sufficient time to the consideration of risk issues. The board of directors shall be actively involved in and ensure that adequate resources are allocated to the management of all material risks addressed in the Act and any regulations and Banking Rules issued thereunder transposing the CRD and in the CRR as well as in the valuation of assets, the use of external credit ratings and internal models relating to those risks. The credit institution shall establish reporting lines to the board of directors that cover all material risks and risk management policies and changes thereof.

62. Credit institutions that are significant shall establish a risk committee composed of directors having a non-executive role in the credit institution concerned. Members of the risk committee shall have appropriate knowledge, skills and expertise to fully understand and monitor the risk strategy and the risk appetite of the credit institution.

63. The risk committee shall advise the board of directors on the credit institution's overall current and future risk appetite and strategy, taking into account all types of risks, to ensure that they are in line with the business strategy, objectives, corporate culture and values of the credit institution. The risk committee shall assist the board of directors in overseeing the implementation of that strategy by senior management. The board of directors shall retain overall responsibility for risks.

64. The risk committee shall review whether prices of liabilities and assets offered to clients take fully into account the credit institution's business model and risk strategy. Where prices do not properly reflect risks in accordance with the

business model and risk strategy, the risk committee shall present a remedy plan to the board of directors.

65. The Authority may allow a credit institution which is not considered significant as referred to in paragraph 62 to combine the risk committee with the audit committee. Members of the combined committee shall have the knowledge, skills and expertise required for the risk committee and for the audit committee.

66. The non-executive directors sitting on the board and, where a risk committee has been established, the risk committee, shall have adequate access to information on the risk situation of the credit institution and, if necessary and appropriate, to the risk management function and to external expert advice.

67. The non-executive directors sitting on the board and, where one has been established, the risk committee shall determine the nature, the amount, the format, and the frequency of the information on risk which it is to receive. In order to assist in the establishment of sound remuneration policies and practices, the risk committee shall, without prejudice to the tasks of the remuneration committee, examine whether incentives provided by the remuneration system take into consideration risk, capital, liquidity and the likelihood and timing of earnings.

68. Without prejudice to the principle of proportionality, credit institutions shall have a risk management function independent from the operational functions and which shall have sufficient authority, stature, resources and access to the board of directors.

69. The risk management function shall ensure that all material risks are identified, measured and properly reported. They shall ensure that the risk management function is actively involved in elaborating the credit institution's risk strategy and in all material risk management decisions and that it can deliver a complete view of the whole range of risks of the credit institution.

70. Where necessary, the risk management function may report directly to the board of directors, independent from senior management, and can raise concerns and warn the board of directors, where appropriate, where specific risk developments affect or may affect the credit institution, without prejudice to the responsibilities of the board of directors pursuant to the Act and any regulations and Banking Rules issued thereunder transposing the CRD and pursuant to the CRR.

71. The head of the risk management function shall be an independent senior manager with distinct responsibility for the risk management function. Where the nature, scale and complexity of the activities of the credit institution do not

justify a specially appointed person, another senior person within the credit institution may fulfil that function, provided there is no conflict of interest.

72. The head of the risk management function shall not be removed without prior approval of the board of directors and shall be able to have direct access to the board of directors where necessary.

73. Where established, the risk committee shall at least:

    a. oversee the implementation of the strategies for capital and liquidity management as well as for all other relevant risks of a credit institution, such as market, credit, operational (including legal and IT risks, in accordance with EU Regulation 2022/2554 on digital operational resilience for the financial sector and EBA Guidelines on ICT and Security Risk Management, EBA/GL/2025/02) and reputational risks, in order to assess their adequacy against the approved risk appetite and strategy;

    b. provide non-executive directors sitting on the board with recommendations on necessary adjustments to the risk strategy resulting from, *inter alia*, changes in the business model of the credit institution, market developments or recommendations made by the risk management function;

    c. provide advice on the appointment of external consultants that the non-executive directors sitting on the board may decide to engage for advice or support;

    d. review a number of possible scenarios, including stressed scenarios, to assess how the credit institution's risk profile would react to external and internal events;

    e. oversee the alignment between all material financial products and services offered to clients and the business model and risk strategy of the credit institution. The risk committee shall assess the risks associated with the offered financial products and services and take into account the alignment between the prices assigned to and the profits gained from those products and services; and

    f. assess the recommendations of internal or external auditors and follow up on the appropriate implementation of measures taken.

74. The risk committee shall collaborate with other committees whose activities may have an impact on the risk strategy (e.g. audit and remuneration committees) and regularly communicate with the credit institution's internal control functions, in particular the risk management function.

75. When established, the risk committee shall, without prejudice to the tasks of the remuneration committee, examine whether incentives provided by the remuneration policies and practices take into consideration the institution's risk, capital and liquidity and the likelihood and timing of earnings.

5.5 Audit Committee

76. Credit institutions shall have an audit committee. The audit committee shall be composed of non-executive directors, and shall have at least three members.

77. The members of the audit committee as a whole shall have competence relevant to the financial sector in which the audited credit institution is operating. At least, the chairperson of the audit committee shall be competent in accounting and/or auditing.

78. The members of the audit committee shall be appointed by the board of directors. The majority of the members of the audit committee shall be independent[1] of the audited credit institution.

79. The chairperson of the audit committee shall, subject to paragraph 78 above, be appointed by the members of the audit committee or by the board of directors and shall be independent of the audited credit institution.

80. Without prejudice to the responsibility of the directors sitting on the board, the audit committee shall, *inter alia*:

    (a) inform the board of directors of the audited credit institution of the outcome of the statutory audit and explain how the statutory audit contributed to the integrity of financial reporting and what the role of the audit committee was in that process;

    (b) monitor the financial reporting process and submit recommendations or proposals to ensure its integrity;

    (c) monitor the effectiveness of the credit institution's internal quality control and risk management systems and, where applicable, its internal audit, regarding the financial reporting of the audited credit institution, without breaching its independence;

[1] For the purposes of this paragraph, a director shall be considered to be independent only if the director sitting on the board is a non-executive member who does not have any management responsibilities within the audited credit institution. This means that such member is free of any business, family, or other relationship ties with such audited credit institution, its controlling shareholders or any member of the group of which the credit institution forms part, and is not under any other undue influence, internal or external, political or ownership, which would impede the board member's exercise of objective judgement.

(d) approve and monitor the internal auditor's work programme, and receive internal audit reports or a periodic summary;

(e) monitor the methods used by senior management to account for significant and unusual transactions where the accounting treatment may be open to different approaches, paying particular attention to both the existence of, and the justification for, any activity carried out by the credit institution in offshore centres and/or through special purpose vehicles;

(f) monitor the responsiveness of senior management to the findings and recommendations of the internal audit function and make recommendations on the selection, appointment, reappointment and removal of the head of the internal audit department and on the department's budget;

(g) monitor the statutory audit of the annual and consolidated financial statements, in particular, its performance, taking into account any findings and conclusions by the Accountancy Board established by the Accountancy Profession Act (Chapter 281 of the Laws of Malta), pursuant to Article 26(6) of Regulation (EU) No 537/2014;[2]

(h) review and monitor the independence of the statutory auditors or the audit firms in accordance with Articles 22, 22a, 22b, 24a and 24b of Directive 2006/43/EC[3] and Article 6 of Regulation (EU) No 537/2014, and in particular the appropriateness of the provision of non-audit services to the audited entity in accordance with Article 5 of Regulation (EU) No 537/2014;

(i) review the statutory auditor's or audit firm's compliance with applicable guidance relating to the rotation of audit partners, the level of fees paid by the credit institution, and other related regulatory requirements;

(j) review the effectiveness of the external audit process, and the responsiveness of senior management to the recommendations made in the statutory auditor's or audit firm's management letter;

[2] Regulation (EU) No 537/2014 of the European Parliament and of the Council of 16 April 2014 on specific requirements regarding statutory audit of public-interest entities and repealing Commission Decision 2005/909/EC.

[3] Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC, as amended by Directive 2008/30/EC of the European Parliament and of the Council of 11 March 2008 amending Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts, as regards the implementing powers conferred on the Commission; Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC; and Directive 2014/56/EU of the European Parliament and of the Council of 16 April 2014 amending Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts; and as may be further amended from time to time.

(k) monitor the statutory auditor's or audit firm's work programme and ensure it obtains timely information about any issues arising from the audit;

(l) be responsible for the procedure for the selection of statutory auditor(s) or audit firm(s) and recommend the statutory auditor(s) or the audit firm(s) to be appointed in accordance with Article 16 of Regulation (EU) No 537/2014;

(m) investigate issues giving rise to any resignation of the statutory auditor or audit firm, and make recommendations as to any required action;

(n) act as the principal point of contact between the internal auditors, the statutory auditor or audit firm and the board of directors in order to ensure that in addition to having an effective working relationship with senior management, both internal and statutory auditors are guaranteed free access to the board of directors;

(o) review the process whereby the credit institution complies with existing provisions regarding the possibility for employees to report alleged significant irregularities in the credit institution, by way of complaints or through anonymous submissions, normally to an independent director, and ensure that arrangements are in place for the proportionate and independent investigation of such matters and for appropriate follow-up action;

(p) decide whether and, if so, when the Chief Executive Officer or Chairperson of the board of directors, the Chief Financial Officer (or senior employees responsible for finance, accounting, and treasury matters), the internal auditor and the statutory auditor or audit firm, should attend its meetings;

(q) be entitled to meet with any relevant person outside the presence of executive and managing directors who do not form part of the audit committee, if it so wishes; and

(r) receive and take into account audit reports.

81. The audit committee shall present the yearly and, if applicable, half-yearly financial statements, to the board of directors for approval.

82. The audit committee shall meet at least quarterly and shall report to the board of directors on its activities:
    (a) at least quarterly in the case of significant credit institutions;
    (b) at least bi-annually in the case of less significant credit institutions.

83. In order to ensure the well-functioning of the audit committee, credit institutions shall, *inter alia*:
    (a) ensure that the audit committee is not prohibited from obtaining advice and assistance from external and independent legal, accounting or other advisors as it deems necessary to carry out its duties, and provide the audit committee with appropriate funding to this effect;
    (b) provide an induction programme for new audit committee members, and subsequent relevant training on an ongoing and timely basis; and
    (c) ensure that all audit committee members are provided with full information relating to the credit institution's specific accounting, financial and operational features.

84. In so far as the requirements relating to the audit committee are concerned, paragraphs 76 to 83 shall be read in conjunction with the Regulation (EU) No 537/2014. Particular consideration should be given to Title III (Articles 16 to 19) of the said Regulation, relating to the appointment of statutory auditors or audit firms and to the transitional provisions set out in Article 41 of the same Regulation.

85. Notwithstanding the provisions pertaining to the requirements of the audit committee set out in the Listing Rules, paragraphs 76 to 84 shall also apply to credit institutions listed on a regulated market. In case of any conflict between the provisions of paragraphs 76 to 84 and the Listing Rules, pertaining to the requirements of the audit committee, a credit institution listed on a regulated market shall comply with the requirements set out in paragraphs 76 to 84.

5.6 Nomination Committee

86. Credit institutions which are significant shall establish a nomination committee composed of directors sitting on the board who do not perform any executive function in the credit institution concerned.

    The nomination committee shall:
    (a) identify and recommend, for the approval of the board of directors or for approval of the general meeting, candidates to fill vacancies of the board of directors, evaluate the balance of knowledge, skills, diversity and experience of the board of directors and prepare a description of the roles and capabilities for a particular appointment, and assess the time commitment expected.

        Furthermore, the nomination committee shall decide on a target for the representation of the underrepresented gender in the board of directors and prepare a policy on how to increase the number of the underrepresented gender in the board of directors in order to meet

that target. The target, policy and its implementation shall be made public in accordance with Article 435(2)(c) of the CRR;

(b) periodically, and at least annually, assess the structure, size, composition and performance of the board of directors and make recommendations to the board of directors with regard to any changes;

(c) periodically, and at least annually, assess the knowledge, skills and experience of individual directors sitting on the board and of the board of directors collectively, and report to the board of directors accordingly;

(d) periodically review the policy of the board of directors for selection and appointment of senior management and make recommendations to the board of directors.

In performing its duties, the nomination committee shall, to the extent possible and on an ongoing basis, take account of the need to ensure that the decision making of the board of directors is not dominated by any one individual or small group of individuals in a manner that is detrimental to the interests of the credit institution as a whole.

The nomination committee shall be able to use any forms of resources that it considers to be appropriate, including external advice, and shall receive appropriate funding to that effect.

5.7 Combined Committees

87. In accordance with paragraph 65 of this Rule, the Authority may allow credit institutions that are less significant to combine the risk committee with, when established, the audit committees as referred to in Article 39 of Directive 2006/43/EC.

88. Where risk and nomination committees are established in less significant credit institutions, they may combine the committees. If they do so, those credit institutions shall document the reasons why they have chosen to combine the committees and how the approach achieves the objectives of the committees.

89. Credit institutions shall at all times ensure that the members of a combined committee possess, individually and collectively, the necessary knowledge, skills and expertise to fully understand the duties to be performed by the combined committee.

Section 6: Regulatory Approval of Individuals Assuming Key Positions

90. Those individuals intending to take up positions enabling them to exercise control and direct the business of a credit institution are subject to prior regulatory approval before taking up such roles, in line with the Authority's ex-ante approach. Such positions include directors and/or members of the management body, as applicable, as well as key function holders. Such individuals are required to complete the dedicated Personal Questionnaire found on the Authority's website and submit it together with any supporting documentation to the Authority so that the latter can conduct its suitability assessment. Such assessment needs to take place at authorisation stage, and whenever an institution intends to appoint or replace an individual to occupy such positions.

91. Credit institutions shall ensure that they comply with the joint ESMA and EBA Guidelines on Suitability Assessment (EBA/GL/2021/06) when proposing and appointing individuals to take up the roles of director and/or member of the management body, and/or key function holder. Institutions deemed to be significant credit institutions in accordance with Council Regulation (EU) No 1024/2013 of 15 October 2013, conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions, shall also make reference to the ECB Guide to fit and proper assessments. In conducting its assessments, the Authority shall also be guided by the afore-mentioned joint ESMA/EBA Guidelines and ECB Guide, as applicable.

92. Credit institutions shall notify the Authority immediately following the resignation of members occupying key positions. Such notification shall include interim arrangements and plans moving forward with respect to the role itself as well as the responsibilities for the necessary decision-making related to this role, thus mitigating the related risks and ensuring the necessary continuity. In this regard, credit institutions are expected to have robust succession plans as outlined in this Rule thus ensuring better continuity once individuals occupying key positions leave their respective roles. On a regular basis, the credit institution shall then report to the Authority on any interim decisions taken and on developments with regards to the recruitment process. In addition to this, separate signed declarations shall be received from the individual resigning and the institution from which the individual resigned. Such declarations shall attest whether this resignation was due to regulatory reasons or otherwise.

93. The Personal Questionnaire shall be submitted at the earliest once an individual has been identified by the institution to assume the vacated position. The proposed person may only assume the role after regulatory approval is received from the Authority, unless otherwise allowed to do so by Authority. Moreover, unless specifically allowed by the Authority, during such period and until formal approval is obtained, all executive decisions are to be taken by another individual, in the next role up, who has already been approved

to occupy such role. In those circumstances where there is no senior role for the vacant position, decisions shall be taken by the relevant Committee or Board.

PART 3 - GOVERNANCE FRAMEWORK - ORGANISATIONAL FRAMEWORK AND STRUCTURE

Section 7: Organisational Framework

94. The board of directors of a credit institution shall ensure a suitable and transparent organisational and operational structure for that credit institution and shall have a written description of it. The structure shall promote and demonstrate the effective and prudent management of a credit institution at individual, sub-consolidated and consolidated levels. The board of directors shall ensure that the internal control functions are independent of the business lines they control, including that there is an adequate segregation of duties, and that they have the appropriate financial and human resources as well as powers to effectively perform their role. The reporting lines and the allocation of responsibilities, in particular among key function holders, within a credit institution shall be clear, well defined, coherent, enforceable and duly documented. The documentation shall be updated as appropriate.

95. The structure of the credit institution shall not impede the ability of the board of directors to oversee and manage effectively the risks that the credit institution or the group faces or the ability of the Authority to effectively supervise the credit institution.

96. The board of directors shall assess whether and how material changes to the group's structure (e.g. setting up of new subsidiaries, mergers and acquisitions, selling or winding-up parts of the group, or external developments) impact on the soundness of the credit institution's organisational framework. Where weaknesses are identified, the board of directors shall make any necessary adjustments swiftly.

Section 8: Know your Structure

97. The board of directors shall fully know and understand the legal, organisational and operational structure of the credit institution ('know your structure') and ensure that it is in line with its approved business and risk strategy and risk appetite and covered by its risk management framework.

98. The board of directors shall be responsible for the approval of sound strategies and policies for the establishment of new structures. Where a credit institution creates many legal entities within its group, their number and, in particular, the interconnections and transactions between them shall not pose

challenges for the design of its internal governance, and for the effective management and oversight of risks of the group as a whole. The board of directors shall ensure that the structure of a credit institution and, where applicable, the structures within a group, taking into account the criteria specified in Section 7 of this Rule, are clear, efficient and transparent to the credit institution's staff, shareholders and other stakeholders and to the competent authority.

99. The board of directors shall guide the credit institution's structure, its evolution and its limitations and shall ensure that the structure is justified and efficient and does not involve undue or inappropriate complexity.

100. The board of directors of a consolidating credit institution shall understand not only the legal, organisational and operational structure of the group but also the purpose and activities of its different entities and the links and relationships among them. This includes understanding group-specific operational risks and intra-group exposures as well as how the group's funding, capital, liquidity and risk profiles could be affected under normal and adverse circumstances. The board of directors shall ensure that the credit institution is able to produce information on the group in a timely manner, regarding the type, the characteristics, the organisational chart, the ownership structure and the businesses of each legal entity, and that the institutions within the group comply with all supervisory reporting requirements on an individual, sub-consolidated basis.

101. The board of directors of a consolidating credit institution shall ensure that the different group entities (including the consolidating credit institution itself) receive enough information to get a clear perception of the general objectives, strategies and risk profile of the group and how the group entity concerned is embedded in the group's structure and operational functioning. Such information and revisions thereof shall be documented and made available to the relevant functions concerned, including the board of directors, business lines and internal control functions. The directors sitting on the board of a consolidating credit institution shall keep themselves informed about the risks the group's structure causes, taking into account the criteria specified in Section 7 of this Rule. This includes receiving:

    a. information on major risk drivers;

    b. regular reports assessing the credit institution's overall structure and evaluating the compliance of individual entities' activities with the approved group-wide strategy; and

    c. regular reports on topics where the regulatory framework requires compliance at individual, sub-consolidated and consolidated levels.

Section 9: Complex Structures and Non-Standard or Non-Transparent Activities

102. Credit institutions shall avoid setting up complex and potentially non-transparent structures. Credit institutions shall take into account in their decision-making the results of a risk assessment performed to identify whether such structures could be used for a purpose connected with money laundering or other financial crimes and the respective controls and legal framework in place. To this end, credit institutions shall take into account at least:

    a. the extent to which the jurisdiction in which the structure will be set up complies effectively with European Union and international standards on tax transparency, anti-money laundering and countering the financing of terrorism;

    b. the extent to which the structure serves an obvious economic and lawful purpose;

    c. the extent to which the structure could be used to hide the identity of the ultimate beneficial owner;

    d. the extent to which the customer's request that leads to the possible setting up of a structure gives rise to concern;

    e. whether the structure might impede appropriate oversight by the credit institution's board of directors or the credit institution's ability to manage the related risk; and

    f. whether the structure poses obstacles to effective supervision by competent authorities.

103. Credit institutions shall not set up opaque or unnecessarily complex structures which have no clear economic rationale or legal purpose or structures that could raise concerns that these might be used for a purpose connected with financial crime.

104. When setting up such structures, the board of directors shall understand them and their purpose and the particular risks associated with them and ensure that the internal control functions are appropriately involved. Such structures shall be approved and maintained only when their purpose has been clearly defined and understood, and when the board of directors is satisfied that all material risks, including reputational risks, have been identified, that all risks can be managed effectively and appropriately reported, and that effective oversight has been ensured. The more complex and opaque the organisational and operational structure, and the greater the risks, the more intensive the oversight of the structure shall be.

105. Credit institutions shall document their decisions and be able to justify their decisions to the Authority.

106. The board of directors shall ensure that appropriate actions are taken to avoid or migrate the risks of activities within such structures. This includes, *inter alia*, ensuring that:

    a. the credit institution has in place adequate policies and procedures and documented processes (e.g. applicable limits, information flows) for the consideration, compliance, approval and risk management of such activities, taking into account the consequences for the group's organisational and operational structure, its risk profile and its reputational risk;

    b. information concerning these activities and the risks thereof is accessible to the consolidating credit institution and internal and external auditors and is reported to the non-executive directors sitting on the board and to the Authority that granted authorisation; and

    c. the credit institution periodically assesses the continuing need to maintain such structures.

107. These structures and activities, including their compliance with legislation and professional standards, shall be subject to regular review by the internal audit function following a risk-based approach.

108. Credit institutions shall take the same risk management measures as for the credit institution's own business activities when they perform non-standard or non-transparent activities for clients (e.g. helping clients to set up vehicles in offshore jurisdictions, developing complex structures, financing transactions for them or providing trustee services) that pose similar internal governance challenges and create significant operational and reputational risks. In particular, credit institutions shall analyse the reason why a client wants to set up a particular structure.

Section 10: Organisational Framework in a Group Context

109. Parent undertakings and subsidiaries subject to the CRD shall ensure that governance arrangements, processes and mechanisms are consistent and well-integrated on a consolidated and sub-consolidated basis. To this end, parent undertakings and subsidiaries within the scope of prudential consolidation shall implement such arrangements, processes and mechanisms in their subsidiaries not subject to the CRD including those established in third countries, including in offshore financial centres, to ensure robust governance arrangements on a consolidated and sub-consolidated basis. With regard to remuneration requirements some exceptions in line with

Articles 109(4) and (5) of the CRD apply. Competent functions within the consolidating credit institution and its subsidiaries shall interact and exchange data and information as appropriate. The governance arrangements, processes and mechanisms shall ensure that the consolidating credit institution has sufficient data and information and is able to assess the group-wide risk profile, as detailed in Section 8.

110. The board of directors of a subsidiary that is subject to the CRD shall adopt and implement on the individual level the group-wide governance policies established at the consolidated or sub-consolidated level, in a manner that complies with all specific requirements under European Union and national law.

111. At the consolidated and sub-consolidated levels, the consolidating credit institution shall ensure adherence to the group-wide governance policies by all credit institutions and other entities within the scope of prudential consolidation, including their subsidiaries not themselves subject to the CRD. When implementing governance policies, the consolidating credit institution shall ensure that robust governance arrangements are in place for each subsidiary and consider specific arrangements, processes and mechanisms where business activities are organised not in separate legal entities but within a matrix of business lines that encompasses multiple legal entities.

112. A consolidating credit institution shall consider the interests of all its subsidiaries, and how strategies and policies contribute to the interest of each subsidiary and the interest of the group as a whole over the long term.

113. Parent undertakings and their subsidiaries shall ensure that the credit institutions and entities within the group comply with all specific requirements in any relevant jurisdiction.

114. The consolidating credit institution shall ensure that subsidiaries established in third countries, and which are included in the scope of prudential consolidation, have governance arrangements, processes and mechanisms in place that are consistent with group-wide governance policies and comply with the requirements of the CRD, as long as this is not unlawful under the laws of the third country.

115. The governance requirements of the CRD and of this Rule apply to credit institutions independent of the fact that they may be subsidiaries of a parent undertaking in a third country. Where an EU subsidiary of a parent undertaking in a third country is a consolidating credit institution, the scope of prudential consolidation does not include the level of the parent undertaking located in a third country and other direct subsidiaries of that parent undertaking. The consolidating credit institution shall ensure that the group-wide governance policy of the parent credit institution in a third country is taken into consideration within its own governance policy insofar as this is not contrary

to the requirements set out under relevant EU law, including the CRD, and this Rule.

116. When establishing policies and documenting governance arrangements, credit institutions shall take into account the following aspects:

In line with Title 2 of this Rule, credit institutions shall consider the following aspects when documenting internal governance policies and arrangements:

a) shareholder structure;
b) group structure, if applicable (legal and functional structure);
c) composition and functioning of the board of directors:
    i. selection criteria;
    ii. number, length of mandate, rotation, age;
    iii. independent directors sitting on the board;
    iv. executive directors sitting on the board;
    v. non-executive directors sitting on the board;
    vi. internal division of tasks, if applicable;

d) governance structure and organisation chart (with impact on the group, if applicable)
e) specialised committees
    i. composition;
    ii. functioning.
f) executive committee, if any
    i. composition;
    ii. functioning key function holders

g) key function holders
    i. head of the risk management function;
    ii. head of the compliance function;
    iii. head of the internal audit function;
    iv. chief financial officer;
    v. other key function holders.

h) internal control framework
    i. description of each function, including its organisation, resources, stature and authority.

i) description of the risk strategy and risk management framework;

j) organisational structure (with impact on the group, if applicable)
    i. operational structure, business lines, and allocation of competences and responsibilities;
    ii. outsourcing;
    iii. range of products and services;
    iv. geographical scope of business;
    v. provision of services under the regime of freedom of provision of services;

vi. branches;
vii. subsidiaries, joint ventures, etc.;
viii. use of offshore centres.

k) code of conduct and behaviour (with impact on the group, if applicable)
   i. strategic objectives and company values;
   ii. internal codes and regulations, prevention policy;
   iii. conflict of interest policy;
   iv. whistleblowing.

l) status of the internal governance policy, with date
   i. development;
   ii. last amendment;
   iii. last assessment;
   iv. approval by the board of directors.

While policies and documentation may be included in separate documents, credit institutions shall consider combining them or referring to them in a single governance framework document.

Section 11: Outsourcing Policy

117. In accordance with paragraph 31 of BR/14 on Outsourcing by Credit Institutions Authorised under the Banking Act, the board of directors shall approve and regularly review and update the outsourcing policy of a credit institution, ensuring that appropriate changes are implemented in a timely manner. Credit institutions shall adhere to the requirements laid out in Section 2.3 of Banking Rule BR/14 with respect to the outsourcing policy.

PART 4 - RISK CULTURE AND BUSINESS CONDUCT

Section 12: Risk Culture

118. A sound and consistent risk culture shall be a key element of credit institutions' effective risk management and shall enable credit institutions to make sound and informed decisions.

119. Credit institutions shall develop an integrated and institution-wide risk culture, based on a full understanding and holistic view of the risks they face and how they are managed, taking into account the credit institution's risk appetite.

120. Credit institutions shall develop a risk culture through policies, communication and staff training regarding the credit institution's activities, strategy and risk profile, and shall adapt communication and staff training to take into account staff's responsibilities regarding risk-taking and risk management.

121. Staff shall be fully aware of their responsibilities relating to risk management. Risk management shall not be confined to risk specialists or internal control functions. Business units, under the oversight of the board of directors, shall be primarily responsible for managing risks on a day-to-day basis in line with the credit institution's policies, procedures and controls, taking into account the credit institution's risk appetite and risk capacity.

122. A strong risk culture shall include but is not necessarily limited to:

    a. tone from the top: the board of directors shall be responsible for setting and communicating the credit institution's core values and expectations. The behaviour of its members shall reflect the values being espoused. Credit institution's management, including key function holders, shall contribute to the internal communication of core values and expectations to staff. Staff shall act in accordance with all applicable laws and regulations and promptly escalate observed non-compliance within or outside the credit institution (e.g. to the Authority through a whistleblowing process). The board of directors shall, on an ongoing basis, promote, monitor and assess the risk culture of the credit institution; consider the impact of the risk culture on the financial stability, risk profile and robust governance of the credit institution; and make changes where necessary;

    b. accountability: relevant staff at all levels shall know and understand the core values of the credit institution and, to the extent necessary for their role, its risk appetite and risk capacity. They shall be capable of performing their roles and be aware that they will be held accountable for their actions in relation to the credit institution's risk-taking behaviour;

    c. effective communication and challenge: the board of directors shall ensure a sound risk culture which promotes an environment of open communication and effective challenge in which decision-making processes encourage a broad range of views, allow for testing of current practices, stimulate a constructive critical attitude among staff, and promote an environment of open and constructive engagement throughout the entire organisation; and

    d. incentives: the board of directors shall ensure that there are in place appropriate incentives that play a key role in aligning risk-taking behaviour with the credit institution's risk profile and its long-term interest.

Section 13: Corporate Values and Code of Conduct

123. The board of directors shall develop, adopt, adhere to and promote high ethical and professional standards, taking into account the specific needs and characteristics of the credit institution, and shall ensure the implementation of such standards (through a code of conduct or similar instrument). It shall also oversee adherence to these standards by staff. Where applicable, the board of directors may adopt and implement the credit institution's group wide standards or common standards released by associations or other relevant organisations.

124. Credit institutions shall ensure that there is no discrimination of staff based on gender, race, colour, ethnic, or social origin, genetic features, language, religion, or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

125. Credit institutions' policies shall be gender neutral. This includes, but is not limited to remuneration, recruitment policies, career development and succession plans, access to training and ability to apply for internal vacancies. Credit institutions shall ensure equal opportunities for all staff independent of their genders, including with regard to career perspectives and aim to improve the representation of the underrepresented gender in positions within the board of directors as well as in the group of staff that have managerial responsibilities as defined in the Commission's Delegated Regulation (regulatory technical standards (RTS) on identified staff). Credit institutions shall monitor the development of the gender pay gap separately for identified staff (excluding directors sitting on the board), executive directors, non-executive directors and other staff. Credit institutions shall have policies that facilitate the reintegration of staff after maternity, paternity or parental leave.

126. The implemented standards shall aim to reduce the risks to which the credit institution is exposed, in particular operational and reputational risks, which can have a considerable adverse impact on a credit institution's profitability and sustainability through fines, litigation costs, restrictions imposed by competent authorities, other financial and criminal penalties and the loss of brand value and consumer confidence.

127. The board of directors shall have clear and documented policies for how these standards shall be met. These policies shall:

    a. remind readers that all the credit institution's activities shall be conducted in compliance with the applicable law and with the credit institution's corporate values;

    b. promote risk awareness through a strong risk culture in line with Section 12 of this Rule, conveying the board of directors' expectation that activities will not go beyond the defined risk appetite and limits defined by the credit institution and the respective responsibilities of staff;

c. set out principles on and provide examples of acceptable and unacceptable behaviours linked in particular to financial misreporting and misconduct, economic and financial crime (including fraud, money laundering and terrorist financing (ML/TF), anti-trust practices, financial sanctions, bribery and corruption, market manipulation, mis-selling and other violations of consumer protection laws, tax offences, whether committed directly or indirectly, including through unlawful or banned dividend arbitrage schemes);

d. clarify that in addition to complying with legal and regulatory requirements and internal policies, staff are expected to conduct themselves with honesty and integrity and perform their duties with due skill, care and diligence; and

e. ensure that staff are aware of the potential internal and external disciplinary actions, legal actions and sanctions that may follow misconduct and unacceptable behaviours.

128. Credit institutions shall monitor compliance with such standards and ensure staff awareness, e.g. by providing training. Credit institutions shall define the function responsible for monitoring compliance with and evaluating breaches of the code of conduct or similar instrument and a process for dealing with issues of non-compliance. The results shall periodically be reported to the board of directors.

Section 14: Conflict of Interest Policy at Institutional Level

129. The board of directors shall be responsible for establishing, approving and overseeing the implementation and maintenance of effective policies to identify, assess, manage and mitigate or prevent actual and potential conflicts of interest at institutional level, e.g. as a result of the various activities and roles of the credit institution, of different credit institutions within the scope of prudential consolidation or of different business lines or units within a credit institution, or with regard to external stakeholders.

130. Credit institutions shall take, within their organisational and administrative arrangements, adequate measures to prevent conflicts of interest from adversely affecting the interests of its clients.

131. Credit institutions' measures to manage or where appropriate mitigate conflicts of interest shall be documented and include, *inter alia*:

a. an appropriate segregation of duties, e.g. entrusting conflicting activities within the processing of transactions or when providing services to different persons, or entrusting supervisory and reporting responsibilities for conflicting activities to different persons;

b. establishing information barriers, e.g. through the physical separation of certain business lines or units; and

c. establishing adequate procedures for transactions with related parties, for example. requiring transactions to be conducted at arm's length in accordance with Banking Rule BR/11 on the Extension of the Applicability of the "Arm's length" Principle by Credit Institutions authorised under the Banking Act 1994.

Section 15: Conflict of Interest Policy for Staff

132. The board of directors shall be responsible for establishing, approving and overseeing the implementation and maintenance of effective policies to identify, assess, manage and mitigate or prevent actual and potential conflicts between the interests of the credit institution and the private interests of staff, including directors sitting on the board, which could adversely influence the performance of their duties and responsibilities. A consolidating credit institution shall consider interests within a group-wide conflict of interest policy on a consolidated or sub-consolidated basis.

133. The policy shall aim to identify conflicts of interest of staff, including the interests of their closest family members. Credit institutions shall take into consideration that conflicts of interest may arise not only from present but also from past personal or professional relationships. Where conflicts of interest arise, credit institutions shall assess their materiality and decide on and implement as appropriate mitigating measures.

134. Regarding conflicts of interest that may result from past relationships, credit institutions shall set an appropriate timeframe for which they want staff to report such conflicts of interest, on the basis that these may still have an impact on staff's behaviour and participation in decision-making.

135. The policy shall cover at least the following situations or relationships where conflicts of interest may arise:

a. economic interests (e.g. shares, other ownership rights and memberships, financial holdings and other economic interests in commercial customers, intellectual property rights, loans granted by the credit institution to a company owned by staff, membership in a body or ownership of a body or entity with conflicting interests);

b. personal or professional relationships with the owners of qualifying holdings in the credit institution;

c. personal or professional relationships with staff of the credit institution or entities included within the scope of prudential consolidation (e.g. family relationships);

d. other employment and previous employment within the recent past (e.g. five years);

e. personal or professional relationships with relevant external stakeholders (e.g. being associated with material suppliers, consultancies or other service providers); and

f. political influence or political relationships.

136. Notwithstanding the above, credit institutions shall take into consideration that being shareholder of a credit institution or having private accounts or loans with or using other services of a credit institution shall not lead to a situation where staff are considered to have a conflict of interest if they stay within an appropriate de minimis threshold.

137. The policy shall set out the processes for reporting and communication to the function responsible under the policy. Staff shall have the duty to promptly disclose internally any matter that may result, or has already resulted, in a conflict of interest.

138. The policy shall differentiate between conflicts of interest that persist and need to be managed permanently and conflicts of interest that occur unexpectedly with regard to a single event (e.g. a transaction, the selection of service provider, etc.) and can usually be managed with a one-off measure. In all circumstances, the interest of the credit institution shall be central to the decision taken.

139. The policy shall set out procedures, measures, documentation requirements and responsibilities for the identification and prevention of conflicts of interest, for the assessment of their materiality and for taking mitigating measures. Such procedures, requirements, responsibilities and measures shall include:

a. entrusting conflicting activities or transactions to different persons;

b. preventing staff who are also active outside the credit institution from having inappropriate influence within the credit institution regarding those other activities;

c. establishing the responsibility of the directors sitting on the board to abstain from voting on any matter where a member has or may have a conflict of interest or where the member's objectivity or ability to properly fulfil duties to the credit institution may be otherwise compromised;

d. establishing adequate procedures for transactions with related parties (credit institutions may consider, *inter alia*, requiring transactions to be conducted at arm's length, requiring that all relevant internal control procedures fully apply to such transactions, requiring binding

consultative advice from independent directors sitting on the board, requiring the approval by shareholders of the most relevant transactions and limiting exposure to such transactions); and

e. preventing directors sitting on the board from holding directorships in competing credit institutions, unless they are within credit institutions that belong to the same institutional protection scheme, as referred to in Article 113(7) of the CRR, credit institutions permanently affiliated to a central body, as referred to in Article 10 of the CRR, or credit institutions within the scope of prudential consolidation.

140. The policy shall specifically cover the risk of conflicts of interest at the level of the board of directors and provide sufficient guidance on the identification and management of conflicts of interest that may impede the ability of directors sitting on the board to take objective and impartial decisions that aim to fulfil the best interest of the credit institution. Credit institutions shall take into consideration that conflicts of interest can have an impact on the independence of mind of directors sitting on the board.

141. When mitigating identified conflicts of interests of directors sitting on the board, credit institutions shall document the measures taken, including the reasoning on how those are effective to ensure objective-decision-making.

142. Actual or potential conflicts of interest that have been disclosed to the responsible function within the credit institution shall be appropriately assessed and managed. If a conflict of interest of staff is identified, the credit institution shall document the decision taken, in particular if the conflict of interest and the related risks have been accepted, and if it has been accepted, how this conflict of interest has been satisfactorily mitigated or remedied.

143. All actual and potential conflicts of interest at board of directors level, individually and collectively, shall be adequately documented, communicated to the board of directors, and discussed, decided on and duly managed by the board of directors.

Section 16: Conflict of Interest Policy in the Context of Loans and Other Transactions with Directors Sitting on the Board and their Related Parties

144. Data on loans to the directors sitting on the board and their related parties shall be properly documented and made available to the Authority upon request.

For the purposes of this paragraph, the term “related party” shall mean:
(a) a spouse, registered partner in accordance with national law, child or parent of a director sitting on the board;

(b) a commercial entity, in which a director sitting on the board or his or her close family member as referred to in point (a) has a qualifying holding of 10% or more of capital or of voting rights in that entity, or in which those persons can exercise significant influence, or in which those persons hold senior management positions or are directors sitting on the board.

145. As part of their conflict of interest policies for staff (Section 15) and the management of conflicts of interest of directors sitting on the board as set out in paragraph 141, the board of directors shall set out a framework for identifying and managing conflicts of interest in the context of granting loans and entering into other transactions (e.g. factoring, leasing, property transactions, etc.) with directors sitting on the board and their related parties.

146. Without prejudice to the Act, regulations made and Rules issued thereunder, credit institutions may consider additional categories of related parties to whom they apply, in whole or in part, the conflicts of interest framework regarding loans and other transactions.

147. The conflicts of interest framework shall ensure that decisions regarding the granting of loans and entering into other transactions with directors sitting on the board and their related parties are taken objectively, without undue influence by conflicts of interests and are as a general principle conducted at arm's length.

148. The board of directors shall set out the applicable decision-making processes for granting loans to and entering into other transactions with directors sitting on the board and their related parties. This framework may provide for a differentiation between standard business transactions entered into in the ordinary course of business and concluded on normal market terms and staff loans and transactions, which are concluded on conditions available to all staff. Furthermore, the conflicts of interest framework and decision-making process may differentiate between material and non-material loans and other transactions, different types of loans and other transactions and the level of actual or potential conflicts of interest they may create.

149. As part of the conflicts of interest framework, the board of directors shall set appropriate thresholds (e.g. per product type, or depending on the conditions) above which the loan or other transaction with a director sitting on the board or its related parties always requires the approval by the board of directors. Decisions on material loans or other material transactions with directors sitting on the board that are not being concluded under normal market terms, but on conditions available to all staff, shall always be made by the board of directors.

150. The director sitting on the board benefitting from such a material loan or other material transaction or the director who is related to the counterparty, shall not be involved in the decision-making.

151. When deciding on a loan or other transaction with a director sitting on the board or their related parties, before taking a decision, institutions shall assess the risk to which the credit institution might be exposed due to the transaction.

152. Where loans are arranged as a line of credit (e.g. overdrafts), the initial decision and amendments thereof shall be documented. Any use of such credit facilities within the agreed limits shall not be considered as a new decision on a loan to a director sitting on the board or their related party. Where an amendment of a line of credit is material in line with the credit institution's policy, a new assessment and decision shall be made.

153. To ensure compliance with their conflict of interest policies, credit institutions shall ensure that all relevant internal control procedures fully apply to loans and to other transactions with directors sitting on the board or their related parties and that an appropriate oversight framework is in place at the level of the non-executive directors.

Section 17: Documentation of Loans to Directors Sitting on the Board and their Related Parties and Additional Information

154. For the purpose of paragraph 14 and 144, credit institutions shall document data on loans to directors sitting on the board and their related parties properly, including at least:

    a. The name of the debtor and their status (i.e. director sitting on the board or related party) and regarding loans to a related party, the director sitting on the board to whom the party is related and then nature of the relationship to the related party;
    b. The type/nature of loan and the amount;
    c. The terms and conditions applicable to the loan;
    d. The date of approval of the loan;
    e. The name of the individual or body and its composition taking the decision to approve the loan and the applicable conditions;
    f. The fact (yes/no) as to whether or not the loan has been granted at market conditions; and
    g. The fact (yes/no) as to whether or not the loan has been granted at conditions available to all staff.

155. Credit institutions shall ensure that the documentation of all loans to directors sitting on the board and their related parties is complete and updated and that the credit institution is able to make available to the Authority the complete documentation in an appropriate format upon request without undue delay.

156. For a loan to a director sitting on the board or their related parties above an amount of €200,000, credit institutions shall be able to provide to the Authority upon request the following additional information:

a. The percentage of the loan and the percentage of the sum of all outstanding amounts of loans towards the same debtor compared to:
    i. The sum of its Tier 1 capital and Tier 2 capital and
    ii. Common equity Tier 1 capital of the credit institution;
b. Whether the loan is part of a large exposure; and
c. The relative weight of the aggregated sum of all outstanding amounts of loans towards the same debtor, calculated as a percentage by dividing the total outstanding amount by the total amount of all outstanding loans to directors sitting on the board and their related parties.

Section 18: Internal Alert Procedures

157. Credit institutions shall put in place and maintain appropriate internal alert policies and procedures for staff to report potential or actual breaches of regulatory or internal requirements, including, but not limited to, those of the CRR and national provisions transposing the CRD, or of internal governance arrangements, through a specific, independent and autonomous channel. It is not necessary for reporting staff to have evidence of a breach; however, they shall have sufficient level of certainty that provides sufficient reason to launch an investigation. Credit institutions shall also implement appropriate processes and procedures that ensure that they comply with their obligations under the national transposition of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union Law.

158. To avoid conflicts of interest, credit institutions shall ensure that it is possible for staff to report breaches outside regular reporting lines (e.g. through the compliance function, the internal audit function or an independent internal whistleblowing procedure). Credit institutions shall ensure that the alert procedures ensure the protection of the personal data of both the person who reports the breach and the natural person who is allegedly responsible for the breach, in accordance with Regulation (EU) 2016/679.

159. The alert procedure shall be made available to all staff within a credit institution.

160. Information provided by staff through the alert procedures shall, if available, be made available to the board of directors and other responsible functions defined within the internal policy. Where required by the staff member reporting a breach, the information shall be provided to the board of directors and other responsible functions in an anonymised way. Credit institutions may also provide for a whistleblowing process that allow information to be submitted in an anonymised way.

161. Credit institutions shall ensure that the person reporting the breach is appropriately protected from any negative impact, e.g. retaliation,

discrimination or other types of unfair treatment. The credit institution shall ensure that no person under the credit institution's control engages in victimisation of a person who has reported a breach and shall take appropriate measures against those responsible for any such victimisation.

162. Credit institutions shall also protect persons who have been reported from any negative effects in case the investigation finds no evidence that justifies taking measures against that person. If measures are taken, the credit institution shall take them in a way that aims to protect the person concerned from unintended negative effects that go beyond the objective of the measure taken.

163. In particular, internal alert procedures shall:

    a. be documented (e.g. staff handbooks);

    b. provide clear rules that ensure that information on the reporting and the reported persons and the breach are treated confidentially, in accordance with Regulation (EU) 2016/679, unless disclosure is required under national law in the context of further investigations or subsequent judicial proceedings;

    c. protect staff who raise concerns from being victimised because they have disclosed reportable breaches;

    d. ensure that the potential or actual breaches raised are assessed and escalated, including as appropriate to the relevant competent authority or law enforcement agency;

    e. ensure, where possible, that confirmation of receipt of information is provided to staff who have raised potential or actual breaches;

    f. ensure the tracking of the outcome of an investigation into a reported breach; and

    g. ensure appropriate record keeping.

Section 19: Reporting of breaches to the Competent Authority

164. The provisions of the Protection of the Whistleblower Act (Cap. 527 of the Laws of Malta) apply to the Authority, which is designated to receive external disclosures from whistleblowers regarding matters, activities or services falling under the regulatory and supervisory competence of the Authority. In establishing effective and reliable mechanisms to enable credit institution's staff to report to the Authority relevant potential or actual breaches of regulatory requirements, including, but not limited to, those of the CRR and

national provisions transposing the CRD, the Authority has set up a Whistleblowing Reports Unit. This Unit is set up in accordance with Article 17(1) of the Protection of the Whistleblower Act. Credit institutions shall also refer to the mechanism regarding reporting of breaches published on the MFSA website for further information.

PART 5 - INTERNAL CONTROL FRAMEWORK AND MECHANISMS

Section 20: Internal Control Framework

165. Credit institutions shall develop and maintain a culture that encourages a positive attitude towards risk control and compliance within the credit institution and a robust and comprehensive internal control framework. Under this framework, credit institutions' business lines shall be responsible for managing the risks they incur in conducting their activities and shall have controls in place that aim to ensure compliance with internal and external requirements. As part of this framework, credit institutions shall have internal control functions with appropriate and sufficient authority, stature and access to the board of directors to fulfil their mission, and a risk management framework.

166. The internal control framework of the credit institution concerned shall be adapted on an individual basis to the specificity of its business, its complexity and the associated risks, taking into account the group context. The credit institutions concerned shall organise the exchange of information necessary in a manner that ensures that each board of directors, business line and internal unit, including each internal control function, is able to carry out its duties. This means, for example, a necessary exchange of adequate information between the business lines and the compliance function and the AML/CFT compliance function where it is a separate control function, at the group level and between the heads of the internal control functions at the group level and the board of directors of the credit institution.

167. Credit institutions shall implement appropriate processes and procedures that ensure that they comply with their obligations in the context of combatting money laundering and terrorist financing. Credit institutions shall assess their exposure to the risk that may be used for the purpose of ML/TF and, where necessary, take mitigating measures to reduce those risks as well as their operational and reputational risks linked to them. Credit institutions shall take measures to ensure that their staff is aware of such ML/TF risks and the impact that ML/TF has on the credit institution and the integrity of the financial system.

168. The internal control framework shall cover the whole organisation, including the board of director's responsibilities and tasks, and the activities of all

business lines and internal units, including internal control functions, outsourced activities and distribution channels.

169. The internal control framework of a credit institution shall ensure:

    a. effective and efficient operations;

    b. prudent conduct of business;
    c. adequate identification, measurement and mitigation of risks;

    d. the reliability of financial and non-financial information reported both internally and externally;

    e. sound administrative and accounting procedures; and

    f. compliance with laws, regulations, supervisory requirements and the credit institution's internal policies, processes, rules and decisions.

Section 21: Implementing an Internal Control Framework

170. The board of directors shall be responsible for establishing and monitoring the adequacy and effectiveness of the internal control framework, processes and mechanisms, and for overseeing all business lines and internal units, including internal control functions (such as risk management, compliance, AML/CFT compliance, where separate from the compliance function, and internal audit functions). Credit institutions shall establish, maintain and regularly update adequate written internal control policies, mechanisms and procedures, which shall be approved by the board of directors.

171. A credit institution shall have a clear, transparent and documented decision-making process and a clear allocation of responsibilities and authority within its internal control framework, including its business lines, internal units and internal control functions.

172. Credit institutions shall communicate those policies, mechanisms and procedures to all staff and every time material changes have been made.

173. When implementing the internal control framework, credit institutions shall establish adequate segregation of duties (e.g. entrusting conflicting activities within the processing of transactions or when providing services to different persons, or entrusting supervisory and reporting responsibilities for conflicting activities to different persons) and establish information barriers, e.g. through the physical separation of certain departments.

174. The internal control functions shall verify that the policies, mechanisms and procedures set out in the internal control framework are correctly implemented in their respective areas of competence.

175. Internal control functions shall regularly submit to the board of directors written reports on major identified deficiencies. These reports shall include, for each new identified major deficiency, the relevant risks involved, an impact assessment, recommendations and corrective measures to be taken. The board of directors shall follow up on the findings of the internal control functions in a timely and effective manner and require adequate remedial actions. A formal follow-up procedure on findings and corrective measures taken shall be put in place.

Section 22: Risk Management Framework

176. As part of the overall internal control framework, the credit institution shall have a holistic institution-wide risk management framework extending across all its business lines and internal units, including internal control functions, recognising fully the economic substance of all its risk exposures. The credit institution shall ensure that the risk management framework enables it to make fully informed decisions on risk-taking. The risk management framework shall encompass on- and off-balance sheet risks as well as actual risks and future risks that the credit institution may be exposed to. Risks shall be evaluated from the bottom up and from the top down, within and across business lines, using consistent terminology and compatible methodologies throughout the credit institution and at consolidated or sub-consolidated level. All relevant risks shall be encompassed in the risk management framework with appropriate consideration of both financial and non-financial risks, including credit, market, liquidity, concentration, operational, IT reputational, legal, conduct, compliance with AML/CFT and other financial crime, ESG, and strategic risks.

177. A credit institution’s risk management framework shall include policies, procedures, risk limits and risk controls ensuring adequate, timely and continuous identification, measurement or assessment, monitoring, management, mitigation and reporting of the risks at the business line, credit institution and consolidate or sub-consolidated levels.

178. A credit institution’s risk management framework shall provide specific guidance on implementation of its strategies. This guidance shall, where appropriate, establish and maintain internal limits consistent with the credit institution’s risk appetite and commensurate with its sound operation, financial strength, capital base and strategic goals. A credit institution’s risk profile shall be kept within these established limits. The risk management framework shall ensure that, whenever breaches of risk limits occur, there is

a defined process to escalate and address them with an appropriate follow-up procedure.

179. The risk management framework shall be subject to independent internal review, e.g. performed by the internal audit function, and reassessed regularly against the credit institution's risk appetite, taking into account information from the risk management function and, where established, the risk committee. Factors that shall be considered include, *inter alia*, internal and external developments, including balance-sheet and revenue changes; any increase in the complexity of the credit institution's business, risk profile or operating structure; geographic expansion; mergers and acquisitions; and the introduction of new products or business lines.

180. When identifying and measuring or assessing risks, a credit institution shall develop appropriate methodologies including both forward-looking and backward-looking tools. The methodologies shall allow for the aggregation of risk exposures across business lines and support the identification of risk concentrations. The tools shall include the assessment of the actual risk profile against the credit institution's risk appetite, as well as the identification and assessment of potential and stressed risk exposures under a range of assumed adverse circumstances against the credit institution's risk capacity. The tools shall provide information on any adjustment to the risk profile that may be required. Credit institutions shall make appropriately conservative assumptions when building stressed scenarios.

181. Credit institutions shall take into consideration that the results of quantitative assessment methodologies, including stress testing, are highly dependent on the limitations and assumptions of the models (including the severity and duration of the shock and the underlying risks). The determination of the level of risk taken shall not be based only on quantitative information or model outputs but shall also comprise a qualitative approach (including expert judgements and critical analysis). Relevant macroeconomic environmental trends and data shall be explicitly addressed to identify their potential impact on exposures and portfolios.

182. The ultimate responsibility for risk assessment lies solely with the credit institution, which, accordingly, shall evaluate its risks critically and shall not rely exclusively on external assessments.

183. Credit institutions shall be fully aware of the limitations of models and metrics and use not only quantitative but also qualitative risk assessment tools (including expert judgement and critical analysis).

184. In addition to the credit institutions' own assessment, credit institutions may use external risk assessments (including external credit ratings or externally purchased risk models). Credit institutions shall be fully aware of the exact scope of such assessments and their limitations.

185. Regular and transparent reporting mechanisms shall be established so that the board of directors, its risk committee, where established, and all relevant units in a credit institutions are provided with reports in a timely, accurate, concise, understandable and meaningful manner and can share relevant information about the identification, measurement or assessment, monitoring and management of risks. The reporting framework shall be well defined and documented.

186. Effective communication and awareness regarding risks and the risk strategy is crucial for the whole risk management process, including the review and decision-making processes, and helps prevent decisions that may unknowingly increase risk. Effective risk reporting involves sound internal consideration and communication of risk strategy and relevant risk data (e.g. exposures and key risk indicators), both horizontally across the credit institution and up and down the management chain.

Section 23: New Products and Significant Changes

187. A credit institution shall have in place a well-documented New Product Approval Policy (NPAP), approved by the board of directors, that addresses the development of new markets, products and services, and significant changes to existing ones, as well as exceptional transactions. The policy shall in addition encompass material changes to related processes (e.g. new outsourcing arrangements) and systems (e.g. IT change processes). The NPAP shall ensure that approved products and changes are consistent with the risk strategy and risk appetite of the credit institution and the corresponding limits, or that necessary revisions are made.

188. Material changes or exceptional transactions may include mergers and acquisitions, including the potential consequences of conducting insufficient due diligence that fails to identify post-merger risks and liabilities; setting up structures (e.g. new subsidiaries or single purpose vehicles; new products; changes to systems or the risk management framework or procedures; and changes to the credit institution’s organisation.

189. A credit institution shall have specific procedures for assessing compliance with these policies, taking into account the input of the risk management function. This shall include a systematic prior assessment and documented opinion by the compliance function for new products or significant changes to existing products.

190. A credit institution’s NPAP shall cover every consideration to be taken into account before deciding to enter new markets, deal in new products, launch a new service, or make significant changes to existing products or services. The NPAP shall also include the definitions of ‘new product/market/business’ and ‘significant changes’ to be used in the organisation and the internal functions to be involved in the decision-making process.

191. The NPAP shall set out the main issues to be addressed before a decision is made. These shall include regulatory compliance; accounting; pricing models; the impact on risk profile, capital adequacy and profitability; the availability of adequate font, back and middle office resources; and the availability of adequate internal tools and expertise to understand and monitor the associated risks. Furthermore, to comply with obligations under the AMLD, credit institutions shall identify and assess the ML/TF risk associated with the new product or business practice, and set out the measures to take to mitigate those risks. The decision to launch a new activity shall clearly state the business unit and individuals responsible for it. A new activity shall not be undertaken until adequate resources to understand and manage the associated risks are available.

192. The risk management function and the compliance function shall be involved in approving new products or significant changes to existing products, processes and systems. Their input shall include a full and objective assessment of risks arising from new activities under a variety of scenarios, of any potential shortcomings in the credit institution's risk management and internal control frameworks, and of the credit institution's ability to manage any new risks effectively. The risk management function shall also have a clear overview of the roll-out of new products (or significant changes to existing products, processes and systems) across different business lines ad portfolios, and the power to require that changes to existing products go through the formal NPAP process.

Section 24: Internal Control Functions

193. The internal control functions shall include a risk management function as set out in Section 25, a compliance function as set out in Section 26, and an internal audit function as set out in in Section 27. The risk management and compliance functions shall be subject to review by the internal audit function. The responsibilities of control functions also include ensuring compliance with AML/CTF requirements.

194. The operational risks of the internal control functions may be outsourced, taking into account the proportionality criteria listed in Title 1, to the consolidating credit institution or another entity within or outside of the group with the consent of the boards of directors of the credit institutions concerned. Even when internal control operational tasks are partially or fully outsourced, the head of the internal control function concerned and the board of directors are still responsible for these activities and for maintaining an internal control function within the credit institution.

195. Without prejudice to national law implementing the AMLD, credit institutions shall assign the responsibility for ensuring the credit institution's compliance with the requirements of that Directive and the credit institution's policies and procedures to a staff member (e.g. head of compliance). Credit institutions

may establish a separate AML/TF compliance function as an independent control function. The person responsible for AML/CFT shall, where necessary, be able to directly report to the board of directors.

24.1 Heads of the Internal Control Functions

196. Heads of internal control functions shall be established at an adequate hierarchical level that provides the head of control function with the appropriate authority and stature needed to fulfil his or her responsibilities. Notwithstanding the overall responsibility of the board of directors, heads of internal control functions shall be independent of the business lines or units they control. To this end, the heads of the risk management, compliance and internal audit functions shall report and be directly accountable to the board of directors, and their performance shall be reviewed by the board of directors.

197. Where necessary, the heads of internal control functions shall be able to have access and report directly to the non-executive directors sitting on the board to raise concerns and warn the non-executive members, where appropriate, when specific developments affect or may affect the credit institution. This shall not prevent the heads of internal control functions from reporting within the regular reporting lines as well.

198. Credit institutions shall have documented processes in place to assign the position of the head of an internal control function and for withdrawing his or her responsibilities. The heads of internal control shall not be removed without the prior approval of the non-executive directors sitting on the board. In significant credit institutions, the Authority shall be promptly informed about the approval and the main reasons for the removal of a head of an internal control function.

24.2 Independence of Internal Control Functions

199. In order for the internal control functions to be regarded as independent, the following conditions shall be met:

    a) their staff do not perform any operational tasks that fall within the scope of the activities the internal control functions are intended to monitor and control;
    b) they are organisationally separate from the activities they are assigned to monitor and control;
    c) notwithstanding the overall responsibility of directors sitting on the board of the credit institution, the head of an internal control function shall not be subordinated to a person who has responsibility for managing the activities the internal control function monitors and controls; and

d) the remuneration of the internal control functions' staff shall not be linked to the performance of the activities the internal control function monitors and controls, and not otherwise likely to compromise their objectivity.

24.3 Combination of Internal Control

200. Taking into account the proportionality criteria set out in Title 1, the risk management function and compliance function may be combined. The internal audit function shall not be combined with another internal control function.

24.4 Resources of Internal Control Functions

201. Internal control functions shall have sufficient resources. They shall have an adequate number of qualified staff (both at parent and at subsidiary level). Credit institutions shall ensure that staff remain qualified on an ongoing basis and receive training as necessary.

202. Internal control functions shall have appropriate IT systems and support at their disposal, with access to the internal and external information necessary to meet their responsibilities. They shall have access to all necessary information regarding all business lines and relevant risk-bearing subsidiaries, in particular those that can potentially generate material risks for the credit institutions.

Section 25: Risk Management Function

203. Credit institutions shall establish a risk management function (RMF) covering the whole credit institution. The RMF shall have sufficient authority, stature and resources, taking into account the proportionality criteria listed in Title 1, to implement risk policies and the risk management framework as set out in Section 25.

204. The RMF shall have, where necessary, direct access to the board of directors and its committees, where established, including in particular the risk committee.

205. The RMF shall have access to all business lines and other internal units that have the potential to generate risk, as well as to relevant subsidiaries and affiliates.

206. Staff within the RMF shall possess sufficient knowledge, skills and experience in relation to risk management techniques and procedures, and markets and products, and shall have access to regular training.

207. The RMF shall be independent of the business lines and units whose risks it controls, however, credit institutions shall not prevent the RMF from interacting with them. Interaction between the operational functions and the RMF shall help to achieve the objective of all the credit institution's staff bearing responsibility for managing risk.

208. The RMF shall be a central organisational feature of the credit institution, structured so that it can implement risk policies and control the risk management framework. The RMF shall play a key role in ensuring that the credit institution has effective risk management processes in place. The RMF shall be actively involved in all material risk management decisions.

209. Significant credit institutions may consider establishing dedicated RMFs for each material business line. However, there shall be a central RMF, including a group RMF in the consolidating credit institution, to deliver a credit institution and group-wide holistic view on all risks and to ensure that the risk strategy is complied with.

210. The RMF shall provide relevant independent information, analyses and expert judgement on risk exposures, and advice on proposals and risk decisions made by business lines or internal units, and shall inform the board of directors as to whether they are consistent with the credit institution's risk appetite and strategy. The RMF may recommend improvements to the risk management framework and corrective measures to remedy breaches of risk policies, procedures and limits.

25.1: RMF's Role in Risk Strategy and Decisions

211. The RMF shall be actively involved at an early stage in elaborating a credit institution's risk strategy and in ensuring that the credit institution has effective risk management processes in place. The RMF shall provide the board of directors with all relevant risk-related information to enable it to set the credit institution's risk appetite level. The RMF shall assess the robustness and sustainability of the risk strategy and appetite. It shall ensure that the risk appetite is appropriately translated into specific risk limits. The RMF shall also assess the risk strategies of business units, including targets proposed by the business units, and shall be involved before a decision is made by the board of directors concerning the risk strategies and risk appetite. Targets shall be plausible and consistent with the credit institution's risk strategy.

212. The RMF's involvement in decision-making processes shall ensure that risk considerations are taken into account appropriately. However, accountability

for the decisions taken shall remain with the business and internal units, and ultimately the board of directors.

25.2: RMF's Role in Material Changes

213. In line with Section 23, before decisions on material changes or exceptional transactions are taken, the RMF shall be involved in the evaluation of the impact of such changes and exceptional transactions on the credit institution's and group's overall risk, and shall report its findings directly to the board of directors before a decision is taken.

214. The RMF shall evaluate how risks identified could affect the credit institution's or group's ability to manage its risk profile, its liquidity and its sound capital base under normal and adverse circumstances.

25.3 RMF's Role in Identifying, Measuring, Assessing, Managing, Mitigating, Monitoring and Reporting on Risks

215. The RMF shall ensure that there is an appropriate risk management framework and that all risks are identified, assessed, measured, monitored, managed and properly reported on by the relevant units in the credit institution.

216. The RMF shall ensure that identification and assessment are not based only on quantitative information or model outputs, but also take into account qualitative approaches. The RMF shall keep the board of directors informed of the assumptions used in and potential shortcomings of the risk models and analysis.

217. The RMF shall ensure that transactions with related parties are reviewed and that the risks they pose for the credit institution are identified and adequately assessed.

218. The RMF shall ensure that all identified risks are effectively monitored by the business units.

219. The RMF shall regularly monitor the actual risk profile of the credit institution and scrutinise it against the credit institution's strategic goals and risk appetite to enable decision-making by the executive directors sitting on the board and challenge by the non-executive directors sitting on the board.

220. The RMF shall analyse trends and recognise new or emerging risks and risk increases arising from changing circumstances and conditions. It shall also regularly review actual risk outcomes against previous estimates (i.e. back testing) to assess and improve the accuracy and effectiveness of the risk management process.

221. The RMF shall evaluate possible ways to mitigate risks. Reporting to the board of directors shall include proposed appropriate risk-mitigating processes.

25.4: RMF's Role in Unapproved Exposure

222. The RMF shall independently assess breaches of risk appetite or limits (including ascertaining the cause and undertaking a legal economic analysis of the actual cost of closing, reducing or hedging the exposure against the potential cost of keeping it). The RMF shall inform the business units concerned and the board of directors, and recommend possible remedies. The RMF shall report directly to the non-executive directors sitting on the board when the breach is material, without prejudice for the RMF to report to other internal functions and committees.

223. The RMF shall play a key role in ensuring a decision on its recommendation is made at the relevant level, complied with by the relevant business units and appropriately reported to the board of directors and, where established, the risk committee.

25.5: Head of the Risk Management Function

224. The head of the RMF shall be responsible for providing comprehensive and understandable information on risks and advising the board of directors, enabling the board to understand the credit institution's overall risk profile. The same applies to the head of the RMF of a parent credit institution regarding the consolidated situation.

225. The head of the RMF shall have sufficient expertise, independence and seniority to challenge decisions that affect a credit institution's exposure to risks. When the head of the RMF is not a director siting on the board, significant credit institutions shall appoint an independent head of the RMF who has no responsibilities for other functions and reports directly to the board of directors. Where it is not proportionate to appoint a person who is dedicated only to the role of head of the RMF, taking into account the principle of proportionality as set out in Title 1, this function can be combined with the head of the compliance function or can be performed by another senior person, provided there is no conflict of interest between the functions combined. In any case, this person shall have sufficient authority, stature and independence (e.g. head of legal).

226. The head of the RMF shall be able to challenge decisions taken by the credit institution's management and its board of directors, and the grounds for objections shall be formally documented. If a credit institution wishes to grant the head of the RMF the right to veto decisions (e.g. a credit or investment decision or the setting of a limit) made at levels below the board of directors,

it shall specify the scope of such a veto right, the escalation or appeal procedures, and how the board of directors will be involved.

227. Credit institutions shall establish strengthened processes for the approval of decisions on which the head of the RMF has expressed a negative view. The non-executive directors sitting on the board shall be able to communicate directly with the head of the RMF on key risk issues, including developments that may be inconsistent with the institution's risk appetite and strategy.

Section 26: Compliance Function

228. Credit institutions shall establish a permanent and effective compliance function to manage compliance risk and shall appoint a person to be responsible for this function across the entire credit institution (the compliance officer or head of compliance).

229. Where it is not proportionate to appoint a person who is dedicated only to the role of head of compliance, taking into account the principle of proportionality as set out in Title 1, this function can be combined with the head of the RMF or can be performed by another senior person (e.g. head of legal), provided there is no conflict of interest between the functions combined.

230. The compliance function, including the head of compliance, shall be independent of the business lines and internal units it controls and have sufficient authority, stature and resources. Taking into account the proportionality criteria set out in Title 1, this function can be combined with the head of the RMF or can be performed by another senior person (e.g. head of legal), provided that there is no conflict of interest between the functions combined.

231. Staff within the compliance function shall possess sufficient knowledge, skills and experience in relation to compliance and relevant procedures, and shall have access to regular training.

232. The non-executive directors sitting on the board shall oversee the implementation of a well-documented compliance policy, which shall be communicated to all staff. Credit institutions shall set up a process to regularly assess changes in the law and regulations applicable to its activities.

233. The compliance function shall advise the board of directors on measures to be taken to ensure compliance with applicable laws, rules, regulations and standards, and shall assess the possible impact of any changes in the legal or regulatory environment on the credit institution's activities and compliance framework.

234. The compliance function shall ensure that compliance monitoring is carried out through a structured and well-defined compliance monitoring programme and that the compliance policy is observed. The compliance function shall report to the board of directors and communicate as appropriate with the RMF on the credit institution's compliance risk and its management. The compliance function and the RMF shall cooperate and exchange information as appropriate to perform their respective tasks. The findings of the compliance function shall be taken into account by the board of directors and the RMF in decision-making processes.

235. In line with Section 23, the compliance function shall also verify, in close cooperation with the RMF and the legal unit, that new products and new procedures comply with the current legal framework and, where appropriate, with any known forthcoming changes to legislation, regulations and supervisory requirements.

236. Credit institutions shall take appropriate action against internal or external fraudulent behaviour and breaches of discipline (e.g. breaches of internal procedures, breaches of limits).

237. Credit institutions shall ensure that their subsidiaries and branches take steps to ensure that their operations are compliant with local laws and regulations. If local laws and regulations hamper the application of stricter procedures and compliance systems implemented by the group, especially if they prevent the disclosure and exchange of necessary information between entities within the group, subsidiaries and branches shall inform the compliance officer or the head of compliance of the consolidating credit institution.

Section 27: Internal Audit Function

238. Credit institutions shall set up an independent and effective internal audit function (IAF), taking into account the proportionality criteria set out in Title 1, and shall appoint a person to be responsible for this function across the entire credit institution. The IAF shall be independent and have sufficient authority, stature and resources. In particular, the credit institution shall ensure that the qualification of the IAF's staff members and the IAF's resources, including its auditing tools and risk analysis methods, are adequate for the credit institution's size and locations, and the nature, scale and complexity of the risks associated with the credit institution's business model, activities, risk culture and risk appetite.

239. The IAF shall be independent of the audited activities. Therefore, the IAF shall not be combined with other functions.

240. The IAF shall, following a risk-based approach, independently review and provide objective assurance of the compliance of all activities and units of a

credit institution, including outsourced activities, with the credit institution's policies and procedures and with external requirements. Each entity within the group shall fall within the scope of the IAF.

241. The IAF shall not be involved in designing, selecting, establishing and implementing specific internal control policies, mechanisms and procedures, and risk limits. However, this shall not prevent the executive directors sitting on the board from requesting input from internal audit on matters related to risk, internal controls and compliance with applicable rules.

242. The IAF shall assess whether the credit institution's internal control framework as set out in Section 20 is both effective and efficient. In particular, the IAF shall assess:

    (a) the appropriateness of the credit institution's governance frameworks;
    (b) whether existing policies and procedures remain adequate and comply with legal and regulatory requirements and with the risk appetite and strategy of the credit institution;
    (c) the compliance of the procedures with the applicable laws and regulations and with decisions of the board of directors;
    (d) whether the procedures are correctly and effectively implemented (e.g. compliance of transactions, the level of risk effectively incurred, etc.); and
    (e) the adequacy, quality and effectiveness of the controls performed and the reporting done by the defence business units and the risk management and compliance functions.

243. The IAF shall verify, in particular, the integrity of the processes ensuring the reliability of the credit institution's methods and techniques, and the assumptions and sources of information used in its internal models (e.g. risk modelling and accounting measurements). It shall also evaluate the quality and use of qualitative risk identification and assessment tools and the risk mitigation measures taken.

244. The IAF shall have unfettered institution-wide access to all the records, documents, information and buildings of the credit institution. This shall include access to management information systems and minutes of all committees and decision-making bodies.

245. The IAF shall adhere to national and international professional standards, an example of the professional standards referred to here is the standards established by the Institute of Internal Auditors.

246. Internal audit work shall be performed in accordance with an audit plan and a detailed audit programme following a risk-based approach.

247. An internal audit plan shall be drawn up at least once a year on the basis of the annual internal audit control objectives. The internal audit plan shall be approved by the board of directors.

248. All audit recommendations shall be subject to a formal follow-up procedure by the appropriate levels of management to ensure and report on their effective and timely resolution.

PART 6 – BUSINESS CONTINUITY MANAGEMENT

249. Credit institutions shall establish a sound business continuity management plan to ensure their ability to operate on an ongoing basis and to limit losses in the event of severe business disruption.

250. Credit institutions may establish a specific independent business continuity function, e.g. as part of the RMF.

251. A credit institution's business relies on several critical resources (e.g. IT systems including cloud services, communication systems and buildings). The purpose of business continuity management is to reduce the operational, financial, legal, reputational, and other material consequences arising from a disaster or extended interruption to these resources and consequent disruption to the credit institution's ordinary business procedures. Other risk management measures might be intended to reduce the probability of such incidents or to transfer their financial impact to third parties (e.g. through insurance).

252. In order to establish a sound business continuity management plan, a credit institution shall carefully analyse risk factors and its exposure to severe business disruptions and assess (quantitatively and qualitatively) their potential impact, using internal and/or external data and scenario analysis. This analysis shall cover all business lines and internal units, including the RMF, and shall take into account their interdependency. The results of the analysis shall contribute to defining the credit institution's recovery priorities and objectives.

253. On the basis of the abovementioned analysis, a credit institution shall put in place:
    a) contingency and business continuity plans to ensure that the credit institution reacts appropriately to emergencies and is able to maintain its most important business activities if there is disruption to its ordinary business procedures; and
    b) recovery plans for critical resources to enable the credit institution to return to ordinary business procedures in an appropriate timeframe. Any residual risk from potential business disruptions shall be consistent with the credit institution's risk appetite.

254. Contingency, business continuity and recovery plans shall be documented and carefully implemented. The documentation shall be available within the business lines, internal units and RMF, and shall be stored on systems that are physically separated and readily accessible in case of contingency. Appropriate training shall be provided. Plans shall be regularly tested and updated. Any challenges or failures occurring in the tests shall be documented and analysed, with the plans reviewed accordingly.

PART 7 - PROVISION OF EQUITY RELEASE FINANCIAL PRODUCTS

255. Credit institutions providing Equity Release Financial Products in accordance with the Equity Release Financial Products Regulations (S.L. 371.21), shall refer to the Equity Release Financial Products Rulebook as may be amended from time to time.

PART 8 - TRANSPARENCY

256. Strategies, policies and procedures shall be communicated to all relevant staff throughout a credit institution. Credit institutions shall ensure that its staff understand and adhere to policies and procedures pertaining to their duties and responsibilities.

257. The board of directors shall inform and update the relevant staff about the credit institution's strategies and policies in a clear and consistent way, at least to the level needed to carry out their particular duties. This may be done through written guidelines, manuals or other means.

258. Where parent undertakings are required by the Authority, as set out under article 30A(2) of the Act, to publish annually a description of their legal structure and governance and the organisational structure of the group of credit institutions, the information shall include all entities within the group structure as defined in the Act, by country.

259. The publication shall include at least:
    a) an overview of the internal organisation of the credit institutions and the group structure and changes thereto, including the main reporting lines and responsibilities;
    b) any material changes since the previous publication and the date of the material change;
    c) new legal, governance or organisational structures;
    d) information on the structure, organisation and directors sitting on the board including the number of its members and the number of those qualified as independent, and specifying the gender and duration of the mandate of each director sitting on the board;

e) the key responsibilities of the board of directors;
f) a list of the committees of the non-executive directors sitting on the board and their responsibilities;
g) an overview of the conflict of interest policy applicable to the credit institutions and to the board of directors;
h) an overview of the internal control framework; and
i) an overview of the business continuity management framework.

PART 9 - TECHNICAL CRITERIA ON GOVERNANCE ARRANGEMENTS AND TREATMENT OF RISKS

Section 28: Internal Approaches[4] for Calculating Own Funds Requirements

260. The Authority encourages credit institutions that are significant to develop internal credit risk assessment capacity and to increase use of the internal ratings based approach for calculating own funds requirements for credit risk where their exposures are material in absolute terms and where they have at the same time a large number of material counterparties. Paragraphs 260 and 261 are without prejudice to the fulfilment of criteria laid down in Part Three, Title II, Chapter 3, Section I of the CRR.

261. In addition to Regulation 14 of the Banking Act (Supervisory Review) Regulations (S.L. 371.16), credit institutions are encouraged to, taking into account their size, internal organisation and the nature, scale and complexity of their activities, develop internal specific risk assessment capacity and to increase use of internal models for calculating own funds requirements for specific risk of debt instruments in the trading book, together with internal models to calculate own funds requirements for default and migration risk where their exposures to specific risk are material in absolute terms and where they have a large number of material positions in debt instruments of different issuers. Paragraphs 260 and 261 are without prejudice to the fulfilment of the criteria laid down in Part Three, Title IV, Chapter 5, Section 1 to 5 of the CRR.

[4] 'Internal Approaches' means the internal ratings based approach referred to in Article 143(1), the internal models approach referred to in Article 221, the own estimates approach referred to in Article 225, the advanced measurement approaches referred to in Article 312(2), the internal models method referred to in Articles 283 and 363, and the internal assessment approach referred to in Article 259(3) of the CRR.

Section 29: Supervisory Benchmarking of Internal Approaches for Calculating Own Funds Requirements

262. Credit institutions permitted to use internal approaches for the calculation of risk weighted exposure amounts or own funds requirements, except for operational risk, shall report the results of the calculations of their internal approaches for their exposures or positions that are included in the benchmark portfolios. Credit institutions shall submit the results of their calculations, together with an explanation of the methodologies used to produce them, to the Authority at an appropriate frequency, and at least annually.

263. Credit institutions shall submit the results of the calculations referred to in paragraph 262 above in accordance with the template developed by the EBA in accordance with the relevant implementing technical standards to the authority and to the EBA. For the supervisory benchmarking of internal approaches for calculating own funds requirements, the Authority shall also refer to Regulation 15 of the Banking Act (Supervisory Review) Regulations.

264. Credit institutions are to refer to any guidelines and recommendations the EBA may issue.

Section 30: Credit and Counterparty Risk

265. Credit-granting shall be based on sound and well-defined criteria. The process for approving, amending, renewing, and re-financing credits shall be clearly established.

266. Credit institutions shall have internal methodologies that enable them to assess the credit risk of exposures to individual obligors, securities or securitisation positions and credit risk at the portfolio level. In particular, internal methodologies shall not rely solely or mechanistically on external credit ratings. Where own funds requirements are based on a rating by an External Credit Assessment Institution (ECAI) or based on the fact that an exposure is unrated, this shall not exempt credit institutions from additionally considering other relevant information for assessing their allocation of internal capital.

267. The ongoing administration and monitoring of the various credit risk-bearing portfolios and exposures of credit institutions, including for identifying and managing problem credits and for making adequate value adjustments and provisions, shall be operated through effective systems.

268. Diversification of credit portfolios shall be adequate, given the credit institution’s target markets and overall credit strategy.

269. Credit institutions engaged in foreign currency lending may be exposed to indirect exchange risk as a component of credit risk though currency mismatches on their customers' balance sheets. To this effect, credit institutions are expected to apply the principles found in MFSA Rule 01/2012 – Foreign Currency Lending Rule through the implementation of appropriate and apposite internal risk management and governance frameworks.

Section 31: Residual Risk

270. The risk that recognised credit risk mitigation techniques used by the credit institution prove less effective than expected shall be addressed and controlled by means of written policies and procedures.

Section 32: Concentration Risk

271. The concentration risk arising from exposures to each counterparty, including central counterparties, groups of connected counterparties, and counterparties in the same economic sector, geographic region or from the same activity or commodity, the application of credit risk mitigation techniques, and including in particular risks associated with large indirect credit exposures such as a single collateral issuer, shall be addressed and controlled including by means of written policies and procedures.

Section 33: Securitisation Risks

272. The risks arising from securitisation transactions in relation to which the credit institutions are investor, originator or sponsor, including reputational risks, such as arise in relation to complex structures or products, shall be evaluated and addressed through appropriate policies and procedures, to ensure that the economic substance of the transaction is fully reflected in the risk assessment and management decisions.

273. Liquidity plans to address the implications of both scheduled and early amortisation shall exist at credit institutions which are originators of revolving securitisation transactions involving early amortisation provisions.

Section 34: Market Risk

274. Policies and processes for the identification, measurement and management of all material sources and effects of market risks shall be implemented.
275. Where the short position falls due before the long position, credit institutions shall also take measures against the risk of a shortage of liquidity.

276. The internal capital shall be adequate for material market risks that are not subject to an own funds requirement.

Credit institutions, which have, in calculating own funds requirements for position risk in accordance with Part Three, Title IV, Chapter 2, of the CRR, netted off their positions in one or more of the equities constituting a stock-index against one or more positions in the stock-index future or other stock-index product shall have adequate internal capital to cover the basis risk of loss caused by the future's or other product's value not moving fully in line with that of its constituent equities. Credit institutions shall also have such adequate internal capital where they hold opposite positions in stock-index futures which are not identical in respect of either their maturity or their composition or both.

Where using the treatment in Article 345 of the CRR, credit institutions shall ensure that they hold sufficient internal capital against the risk of loss which exists between the time of the initial commitment and the following working day.

Section 35: Interest Rate Risk Arising from Non-Trading Activities

277. Credit institutions shall implement internal systems, use the standardised methodology or the simplified standardised methodology to identify, evaluate, manage and mitigate the risks arising from potential changes in interest rates that affect both the economic value of equity and the net interest income of a credit institution’s non-trading book activities.

278. Credit institutions shall implement systems to assess and monitor the risks arising from potential changes in credit spreads that affect both the economic value of equity and the net interest income of a credit institution’s non-trading book activities.

279. A credit institution may be required by the Authority to use the standardised methodology referred to in paragraph 277 where the internal systems implemented by that credit institution for the purpose of evaluating the risks referred to in that paragraph are not satisfactory.

280. The Authority may require a small and non-complex credit institution as defined in point (145) of Article 4(1) of the CRR to use the standardised methodology where it considers that the simplified standardised methodology is not adequate to capture interest rate risk arising from non-trading book activities of that credit institution.

281. Credit institutions are to be guided by any draft regulatory standards issued by the EBA to specify, for the purposes of these paragraphs, a standardised methodology that credit institutions may use for the purpose of evaluating the risks referred to in paragraph 277, including a simplified standardised

methodology for small and non-complex credit institutions as defined in point (145) of Article 4(1) of the CRR which is at least as conservative as the standardised methodology.

Section 36: Operational Risk

282. Credit institutions shall implement policies and processes to evaluate and manage the exposures to operational risk, including model risk and risks resulting from outsourcing, and to cover low-frequency high-severity events. Credit institutions shall articulate what constitutes operational risk for the purposes of those policies and procedures.

283. Contingency and business continuity policies and plans shall be in place, including ICT business continuity policies and plans and ICT response and recovery plans for the technology they use for the communication of information, and that those plans are established, managed and tested in accordance with Article 11 of EU Regulation 2022/2554, to ensure a credit institution's ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

Section 37: Liquidity Risk

284. Credit institutions shall have robust strategies, policies, processes and systems for the identification, measurement, management and monitoring of liquidity risk over an appropriate set of time horizons, including intra-day, so as to ensure that credit institutions maintain adequate levels of liquidity buffers. Those strategies, policies, processes and systems shall be tailored to business lines, currencies, branches and legal entities and shall include adequate allocation mechanisms of liquidity costs, benefits and risks.

285. The strategies, policies, processes and systems referred to in paragraph 284 shall be proportionate to the complexity, risk profile, scope of operation of the credit institutions and risk tolerance set by the board of directors and reflect the credit institution's importance in each Member State in which it carries out business. Credit institutions shall communicate risk tolerance to all relevant business lines.

286. Credit institutions shall, taking into account the nature, scale and complexity of their activities, have liquidity risk profiles that are consistent with and, not in excess of, those required for a well-functioning and robust system. In this regard, the Authority monitors and takes action on developments regarding liquidity risk profiles in accordance with Regulation 10(3) to (5) of the Banking Act (Supervisory Review) Regulations.

287. Credit institutions shall develop methodologies for the identification, measurement, management and monitoring of funding positions. Those methodologies shall include the current and projected material cash-flows in and arising from assets, liabilities, off-balance sheet items, including contingent liabilities and the possible impact of reputational risk.

288. Credit institutions shall distinguish between pledged and unencumbered assets that are available at all times, in particular during emergency situations. They shall also take into account the legal entity in which assets reside, the country where assets are legally recorded either in a register or in an account as well as their eligibility and shall monitor how assets can be mobilised in a timely manner.

289. Credit institutions shall also have regard to existing legal, regulatory and operational limitations to potential transfers of liquidity and unencumbered assets amongst entities, both within and outside the EEA.

290. Credit institutions shall consider different liquidity risk mitigation tools, including a system of limits and liquidity buffers in order to be able to withstand a range of different stress events and an adequately diversified funding structure and access to funding sources. Those arrangements shall be reviewed regularly.

291. Credit institutions shall consider alternative scenarios on liquidity positions and on risk mitigants and review the assumptions underlying decisions concerning the funding position at least annually. For these purposes, alternative scenarios shall address, in particular, off-balance sheet items and other contingent liabilities, including those of Securitisation Special Purpose Entities (SSPE) or other special purpose entities, as referred to in the CRR, in relation to which the credit institution acts as sponsor or provides material liquidity support.

292. Credit institutions shall consider the potential impact of credit institution-specific, market-wide and combined alternative scenarios. Different time periods and varying degrees of stressed conditions shall be considered.

293. Credit institutions shall adjust their strategies, internal policies and limits on liquidity risk and develop effective contingency plans, taking into account the outcome of the alternative scenarios referred to in paragraph 291.

294. Credit institutions shall have in place liquidity recovery plans setting out adequate strategies and proper implementation measures in order to address possible liquidity shortfalls, including in relation to branches established in another Member State. Such plans shall be tested by the credit institutions at least annually, updated on the basis of the outcome of the alternative scenarios set out in paragraph 291, reported to and approved by senior management, so that internal policies and processes can be adjusted accordingly. Credit institutions shall take the necessary operational steps in

advance to ensure that liquidity recovery plans can be implemented immediately. For credit institutions, such operational steps shall include holding collateral immediately available for central bank funding. This includes holding collateral where necessary in the currency of another Member State, or the currency of a third country to which the credit institution has exposures, and where operationally necessary within the territory of a host Member State or of a third country to whose currency it is exposed.

295. The authority recognises that the US Dollar has proven to be a material funding currency for certain credit institutions, and throughout the past years, there have been on-going strains in the US Dollar funding markets. These strains may create key direct potential system-wide risks, in particular material maturity mismatches between the US Dollar assets and liabilities of a credit institution, where short-term funding is used to finance longer term assets in the said currency.

296. Accordingly, the authority requires credit institutions, particularly those which utilise the US Dollar as a material funding currency for their operations, to apply the provisions of MFSA Rule 02/2012 on US Dollar Funding outlines the general principles regulating US Dollar denominated funding.

Section 38: Risk of Excessive Leverage

297. Credit institutions shall have policies and processes in place for the identification, management and monitoring of the risk of excessive leverage. Indicators for the risk of excessive leverage shall include the leverage ratio determined in accordance with Article 429 of the CRR and mismatches between assets and obligations.

298. Credit institutions shall address the risk of excessive leverage in a precautionary manner by taking due account of potential increases in the risk of excessive leverage caused by reductions of the credit institution's own funds through expected or realised losses incurred in accordance with statutory IFRS. To that end, credit institutions shall be able to withstand a range of different stress events with respect to the risk of excessive leverage.

Section 39: ICT and Security Risk

299. Credit institutions shall comply with EU Regulation 2022/2554 on digital operational resilience for the financial sector and the provisions set out in the EBA Guidelines on ICT and Security Risk management (EBA/GL/2025/02).

Malta Financial Services Authority

Triq L-Imdina, Zone 1

Central Business District, Birkirkara, CBD 1010, Malta

communications@mfsa.mt

www.mfsa.mt