

CHAPTER 2 OF THE FINANCIAL INSTITUTIONS RULEBOOK - FIR/02

Rules applicable to financial institutions carrying out any activity listed in the First Schedule to the financial institutions act except for activities 4 (payment services) and, or 10 (issuing of electronic money)

CONTENTS

TITLE 1 GENERAL	1
R2-1.1 INTRODUCTION & SCOPE	1
R2-1.2 DEFINITIONS.....	2
R2-1.3 HIGH LEVEL PRINCIPLES.....	5
R2-1.4 REGULATORY REQUIREMENTS.....	7
TITLE 2 SUPERVISORY REQUIREMENTS OF LICENSED INSTITUTIONS.....	8
R2-2.1 INTRODUCTION.....	8
R2-2.2 MATTERS REQUIRING NOTIFICATION	9
R2-2.3 MATTERS REQUIRING PRIOR APPROVAL	10
R2-2.4 APPROVAL AND DEPARTURE PROCESS FOR APPOINTED PERSONS.....	11
R2-2.5 REQUIREMENTS RELATING TO SOUND & PRUDENT MANAGEMENT	13
R2-2.6 OUTSOURCING REQUIREMENTS	26
R2-2.7 ACCOUNTING AND STATUTORY AUDIT REQUIREMENTS	41
R2-2.8 REPORTING REQUIREMENTS	41
R2-2.9 RECORD KEEPING	44
R2-2.10 LIQUIDITY.....	45
R2-2.11 ICT AND SECURITY RISK	45
R2-2.12 ARM'S LENGTH PRINCIPLE	46
R2-2.13 THIRD PARTY EXPOSURE THRESHOLD	47
R2-2.14 CAPITAL REQUIREMENTS.....	48
R2-2.15 CREDIT RISK MANAGEMENT FRAMEWORK	49
R2-2.16 COMPLAINTS HANDLING	50

REVISIONS LOG

VERSION	DATE ISSUED	DETAILS
1.00	2011	Publishing of supervisory and regulatory requirements
2.00	2019	Amendments to incorporate transposition of Directive 2015/2366
3.00	2020	Amendment to paragraph 48 and the introduction of paragraph 48A regarding the MFSA Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements.
4.00	2025	Amendment to paragraph 48 and paragraph 48A
5.00	2026	Publishing of new supervisory and regulatory requirements amending previous versions

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

SUPERVISORY AND REGULATORY REQUIREMENTS OF INSTITUTIONS AUTHORISED UNDER THE FINANCIAL INSTITUTIONS ACT 1994

Title 1 General

R2-1.1 INTRODUCTION & SCOPE

- R2-1.1.1 This Chapter contains ongoing requirements applicable to Financial Institutions licenced in terms of the Financial Institutions Act ('the Act') and authorised to undertake the following financial institution activities as listed in the First Schedule to the Act with the exception of activity 4 (Payment Services) and/or activity 10 (issuing of Electronic Money).
- R2-1.1.2 In terms of Article 13(2) of the Financial Institutions Act 1994 ('the Act') the competent authority ('the Authority') as appointed under Article 3 of the Malta Financial Services Authority Act may make Financial Institutions Rules as may be required for the carrying into effect of any of the provisions of the Act. The Financial Institutions Rules and any amendment or revocation thereof shall be officially communicated to financial institutions, and the Authority shall make copies thereof available to the public, through publication on the Authority's website.
- R2-1.1.3 The Supervisory and Regulatory Requirements of Institutions Authorised under the Financial Institutions Act 1994 Rule ('the Rule') is being issued in terms of Article 13(4) of the Act which empowers the Authority to provide for different regulatory requirements applicable to different classes of institutions. The requirements in the Rule are of a general nature, and the Authority will apply particular requirements to specific classes of institutions as it deems appropriate through the licence.
- R2-1.1.4 The Rule also highlights the supervisory and investigative powers of the Authority as provided for in the Act. These highlights should not however be construed in any way to be a substitute for a reading of the relevant provisions of the Act itself. The responsibility for observing such provisions rests entirely with the financial institution, its Board of Directors and its management.

R2-1.1.5 This Chapter is not intended to provide a complete summary of the Act, regulations or rules issued thereunder. Therefore, it must not be construed as being a substitute for a reading of the applicable regulatory framework. Licence Holders shall refer to the Act, the regulations issued thereunder, applicable rules issued by the Authority and any other relevant legal and regulatory requirements.

The Licence Holder is also expected to take due account and, where applicable, comply with any relevant local and EU Regulations and Directives. These include but are not limited to:

- i. Central Bank of Malta [Directives](#);
- ii. the [Prevention of Money Laundering Act](#) and subsidiary legislation;
- iii. the [Companies Act](#) (Cap. 386 of the Laws of Malta) and subsidiary legislation emanating therefrom;
- iv. the [Civil Code](#) (Cap. 16 of the Laws of Malta);

In addition, the Authority expects the Licence Holder, where appropriate, to refer to any relevant Commission Delegated Regulations and Directives, Regulatory Technical Standards and Implementing Technical Standards, as well as any Guidelines which may be issued by the EBA to ensure best practice.

R2-1.1.6 This Chapter shall also be read in conjunction with Chapter 1 of the Financial Institutions Rulebook (FIR/01) which sets out the authorisation and registration processes for financial institutions. In particular, FIR01 includes processes relating to:

- modification of licence
- change in participation or control
- surrender of authorisation/ cessation of business

R2-1.1.7 Title 2 of this Chapter outlines the ongoing requirements applicable to all Licence Holders as defined herein.

R2-1.1.8 Title 3 of this Chapter provides for enforcement and sanctions in the event of misconduct by Licence Holders as defined herein.

R2-1.2 Definitions

For the purposes of this Chapter, the definitions set out below shall apply.

In the event that any of the definitions contained herein conflict with a definition under the Act or any other law administered by the Authority for the time being in force in Malta, the definitions set out in the Act shall prevail, unless otherwise specified herein.

Banking Act	means the Banking Act , Chapter 371 of the Laws of Malta;
Central Bank of Malta (CBM)	shall have the meaning as assigned to it under Article 2(1) of the Act;
Clients	means any person, including potential clients, to whom a Licence Holder provides or intends to provide a service as referred to in the First Schedule to the Act;
Directive 2013/36/EU (CRD)	shall have the meaning as assigned to it under Article 2(1) of the Act;
Dual-Licenced	Shall mean a Licence Holder also authorised as a Crypto-Asset Service Provider as defined in point (15) of Article 3(1) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulations (EU) No.1093/2010 and (EU) No. 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (MiCA Regulation);
European Banking Authority (EBA)	shall have the meaning as assigned to it under Article 2(1) of the Act;
Executive Director	means a director who is contractually engaged to undertake the day-to-day executive management and decision-making process of the entity;
Financial Intelligence Analysis Unit (FIAU)	means the Financial Intelligence Analysis Unit as established by the Prevention of Money Laundering Act (Cap. 373 of the Laws of Malta);
Financial Institutions Act or 'the Act'	means the Financial Institutions Act , Chapter 376 of the Laws of Malta;
Financial Institutions Act (Fees) Regulations	means the Financial Institutions (Fees) Regulations , Subsidiary Legislation 376.03 of the Laws of Malta;
Funds	shall have the meaning as assigned to it under Article 2(1) of the Act;
FIR/01	means Chapter 1 of the Financial Institutions Rulebook;
Independent Non-Executive Director	means a Non-Executive Director who is free from any present and past business, family, or other relationship of any nature, with the entity, its controlling shareholder/s or

the management of either, that could influence the Director's objective and balanced judgment and reduce the member's ability to take decisions independently;

Key Function Holder	means persons who have significant influence over the direction of the Licence Holder 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 the Authority, other key function holders. Other key function holders might include heads of significant business lines, the Compliance Officer and the MLRO;
Licence Holder	shall mean a Financial Institution licenced in terms of the Act and authorised to provide activities listed in the First Schedule of the Act with the exception of activity 4 (Payment Services) and/or activity 10 (issuing of Electronic Money);
MFSA or 'the Authority'	means the Malta Financial Services Authority as established by the Malta Financial Services Authority Act , Chapter 330 of the Laws of Malta;
Non-Executive Director	means a director who is not engaged in the daily management of the entity;
Outsourcing	shall have the meaning as assigned to it under Article 2(1) of the Act;
Outsourcing Service Provider	shall have the meaning as assigned to it under Article 2(1) of the Act;
Regulated Activities	refers to the activities set out in the First Schedule of the Act ;
Regulation (EU) No 575/2013 (CRR)	means Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012;
Regulation (EU) 2016/679 (GDPR)	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data,

and repealing Directive 95/46/EC (General Data Protection Regulation);

Senior Management shall refer to those natural persons who exercise executive functions within the Licence Holder and who are responsible and accountable to the Board for the day-to-day management of the Licence Holder;

R2-1.3 High Level Principles

R2-1.3.1 Pursuant to Article 5(1)(d) of the Act the Licence Holder shall act in an ethical and prudent manner taking into consideration the best interests of their clients and the integrity of Malta's financial system.

R2-1.3.2 The Licence Holder shall act honestly, fairly and professionally and shall comply with the relevant provisions of the Act and any applicable regulations and rules issued thereunder, as well as with other relevant legal and regulatory requirements.

R2-1.3.3 Licence Holders shall co-operate with the MFSA in an open and honest manner and shall provide the Authority with any information, documentation, and/ or returns it may require.

R2-1.3.4 Without prejudice to Article 22 of the Act, the Licence Holder and their representatives shall:

- i. make reference to, and where applicable comply with, the applicable Maltese laws, regulations and rules issued thereunder as well as any guidelines which may be issued by the MFSA or other relevant body to assist the said persons in complying with their legal and regulatory obligations;
- ii. cooperate in an open and honest manner with the MFSA and any other relevant regulatory authorities, including the FIAU and the CBM; and

take due account and, where applicable, comply with any relevant EU legislation as well as any guidelines/statements/ industry best practices which may

be issued by international standard setting bodies including any guidelines or guidance notes issued by the FIAU.

- R2-1.3.5 Where documentation is required to be submitted to the Authority and such documentation is signed using a valid qualified signature in accordance with the [circular](#) issued by the MFSA on the use of electronic signatures dated 15 November 2022, the Licence Holder is not required to submit such documentation in original.
- R2-1.3.6 The MFSA expects the Licence Holder to utilise the LH Portal when submitting information and/or documentation to the MFSA pursuant to these the Rule.
- R2-1.3.7 Without prejudice to Article 5 of the Act and to the generality of consideration as to whether the business is being conducted prudently, a licenced financial institution shall not be regarded as conducting its business in a prudent manner unless:
- (a) the directors include non-executive directors as the Authority considers appropriate having regard to the nature and scale of operations of the Licence Holder and who shall act in a control capacity in questioning the approach of the executive directors and other management;
 - (b) every person who is a director, controller, partner or any other officer of the institution is a fit and proper person to hold that particular position and to carry out business with integrity and skill. Without prejudice to Article 24 of the Act, in assessing whether a person has the relevant competence, soundness of judgement and diligence, the Authority considers the experience of similar responsibilities, qualifications and training;
 - (c) its officers take all reasonable steps to ensure that the institution, at all times, adapts itself to the requirements of the relevant Rules or regulations issued under the Act and the provisions of the Act itself;
 - (d) it makes adequate provisions for depreciation or diminution in the value of its assets, for liabilities which will or may fall to be discharged by it and for losses which

it will or may incur. In assessing the adequacy of an institution's provisions, the Authority, where necessary, shall regard that institution's provisioning policies including, when applicable, the methods and systems for monitoring recoverability of loans and other advances and its policies and practices for the taking and valuation of security.; and

- (e) it maintains adequate accounting and other records and adequate systems of control of its business and records that are commensurate with its needs and particular circumstances in such a way as to enable the business of the institution to be prudently managed and for it to comply with the duties imposed on it by or under the Act. In assessing this adequacy, the Authority when appropriate, shall take into consideration the internal audit procedures of the institution.

R2-1.3.8 The Licence Holder shall ensure that its corporate profile on the LH Portal is maintained up to date at all times.

R2-1.4 Regulatory Requirements

R2-1.4.1 The Authority can provide for different regulatory requirements applicable to different classes of institutions. The subsequent paragraphs are intended to establish certain regulatory parameters which may be applied by the Authority on a case-by-case basis as it may deem appropriate in licensing an institution.

R2-1.4.2 Certain services which can be provided by an institution licenced under the Act are similar to those carried out by a credit institution licenced under the Banking Act 1994. Therefore, in the Authority's opinion, institutions licenced to carry out such activities could be considered as quasi-banking institutions. Consequently, it would be prudent, for the safeguarding of the financial system that, to the extent necessary, such institutions are regulated on the same level as credit institutions, without being significantly bound by the provisions of the Banking Act 1994 whilst taking into consideration the fact that at law financial institutions are prohibited from funding their activities through deposits.

R2-1.4.3 A financial institution which is a subsidiary of a credit institution or the parent undertaking of a credit institution or which is part of a group

which also comprises a credit institution would, in the Authority's opinion, require to be regulated within the parameters of a credit institution itself. However, this does not mean that such a financial institution is in any way bound by the provisions of the Banking Act 1994.

- R2-1.4.4 A financial institution carrying out activities listed in the First Schedule to the Act which, although not requiring a licence under the Investment Services Act 1994, are very similar to activities under that Act, may be required to be regulated within the parameters of the said Investment Services Act 1994. The extent to which such requirements will be applied to these institutions will be discussed and agreed by the Authority and the applicant for a licence. The Authority's decision in this respect would however be final.
- R2-1.4.5 Other institutions carrying out activities listed in the First Schedule to the Act which in the Authority's opinion could not be considered as similar to those institutions in R2-1.4.2 to R2-1.4.4 above would require a prudential supervisory approach proportionate to the nature, scale and extent of such activities.

Title 2 SUPERVISORY REQUIREMENTS OF LICENCED INSTITUTIONS

R2-2.1 Introduction

- R2-2.1.1 The Authority places great importance to the timely and accurate reporting of statutory prudential statistical information by financial institutions. Such information, which is to be submitted in terms of Article 14 of the Act, is necessary for supervisory and regulatory reasons.
- R2-2.1.2 All financial institutions are subject to the Authority's continuing prudential supervisory oversight under the Act and Rules. The Authority may conduct its supervision on an individual (solo) or consolidated basis taking account of the operations of banking and other financial companies connected to the licenced institutions always having regard to the individual structure and circumstances of each licenced institution.
- R2-2.1.3 The Authority can exercise its supervisory powers under Article 14 of the Act by appointing competent persons to investigate and report on the affairs of a

financial institution. In this respect the Authority expects all officers of the institution to comply with the provisions of Articles 14, 15, and 16 of the Act.

R2-2.1.4 The Licence Holder shall not take deposits or other repayable funds from the public as per Article 2A of the Banking Act.

R2-2.1.5 The Licence Holder shall be prohibited from undertaking transactions referred to in Article 10 of the Act.

R2-2.2 Matters Requiring Notification

R2-2.2.1 The Licence Holder shall notify the MFSA, via the LH Portal, immediately upon becoming aware, of:

- i. without prejudice to the approval and departure process set out in R2-2.4, any changes in Senior managers and/or Key Function Holders of the Licence Holder;
- ii. any changes in non-qualifying shareholders shall be notified;
- iii. any evidence of significant fraud or dishonesty by a member of the Licence Holder's staff either committed against one of its customers or impinging on the integrity of a staff member;

Provided that significance shall be determined by:

- a. the aggregate size of the monetary loss or potential monetary loss to the Licence Holder or its customers;
- b. the risk of reputational loss to the firm;
- c. whether the incident or a pattern of incidents reflects a weakness in the Licence Holder's internal controls.
- iv. any actual or intended legal or judicial proceedings of a material nature by or against the Licence Holder and/or the ultimate beneficial owners, immediately after the decision has been taken or on becoming aware of the matter.
- v. any other material information concerning the Licence Holder, its business or its staff in Malta or abroad, immediately upon becoming aware of the matter.

Provided that information would be considered material where:

- a. there is a financial impact on the Licence Holder and/or its clients;

- b. there is a reputational impact to the Licence Holder.
- vi. any breach of the Act, regulations, and rules issued thereunder, as soon as the Licence Holder becomes aware of the breach.
- vii. any change to important operational outsourcing arrangements including any changes to the activities which are outsourced and changes in outsourcing service providers pursuant to R2-2.7.9 and R2-2.7.10.
- viii. any change in the responsibilities of an appointed person as defined in R2-2.4.1.
- ix. a decision to open a branch in Malta.

R2-2.2.2 The Licence Holder shall notify the MFSA via the LH Portal, at least 60 calendar days prior, of any change to important operational outsourcing arrangements including any changes to the activities which are outsourced and changes in outsourcing service providers pursuant to R2-2.6.9 and R2-2.6.10.

R2-2.3 Matters Requiring Prior Approval

R2-2.3.1 The Licence Holder shall obtain the written consent of the MFSA before:

- i. implementing material changes to its business or organisational structure at least one month before the change is to take effect, notwithstanding whether the proposed material change/s require authorisation or otherwise, including any decision to undertake additional activities pursuant to Article 5(6) of the Act or to make material changes to the Board of Directors of the Licence Holder.
- ii. agreeing to sell or dispose of its business or any significant part thereof, merge with any other company, undergo any reconstructions or vary its nominal or issued share capital, or effect any material change in the voting rights of its immediate qualifying shareholder.
- iii. the appointment of persons referred to in R2-2.4.
- iv. any decision to open a branch, outside Malta, prior to opening said branch, pursuant to Article 8(2) of the Act.
- v. any decision to acquire or set up a subsidiary in or outside Malta, pursuant to Article 8(2B) of the Act.
- vi. any decision to provide services through an agent.

- vii. the proposed change in the participation in control of the Licence Holder pursuant to Article 9 of the Act in line with the approval processes set out in FIR/01 and R2-2.4 as applicable.
- viii. the governance structure as agreed upon with the Authority at authorisation stage shall be maintained on an on-going basis by the Institution and the latter shall not deviate from this unless seeking prior approval from the authority.
- ix. making a change to its name (including commercial and trade names) and/or address (registered, business, or both).
- x. Any changes to the Own Funds requirement.

R2-2.3.2 Pursuant to R2-2.3.1 point (ii), in requesting the Authority's written consent, the Licence Holder shall submit:

- a. a transition plan for the proposed Board; and
- b. an updated business plan.

R2-2.4 Approval and Departure Process for Appointed Persons

R2-2.4.1 The Licence Holder shall ensure that Appointed Persons follow the approval and departure requirements set out in this section.

For the purposes of this Chapter:

- i. Appointed Persons shall refer to any person who has submitted a Personal Questionnaire and who has been approved by the Authority to hold a specific role/s with the Licence Holder; and
- ii. Proposed Persons shall refer to any person who has been proposed to hold the role of an Appointed Person with the Licence Holder.

Without prejudice to the generality of the foregoing, the following listed persons are required to obtain the Authority's approval prior to commencing their involvement with the Licence Holder:

- ultimate beneficial owners;
- qualifying shareholders;
- directors;
- key function holders.

R2-2.4.2 There are two processes relating to appointed persons, namely (i) the approval process and (ii) the departure process.

R2-2.4.3 Proposed persons shall adhere to the MFSA's [Guidelines to the Personal Questionnaire](#) and submit any documentation to the Authority through the

chat box function within the Authority's LH Portal. Any documentation requested in original should be submitted to the Authority in writing.

- R2-2.4.4 The MFSA shall use all the information provided by the proposed person, and any other information that ought to have been disclosed by the said person for the purposes of the processes referred to in this section. The MFSA shall not be liable in damages for any acts or omissions on the part of the proposed person.

The Approval Process

- R2-2.4.5 Proposed persons appointed or designated in relation to the Licence Holder, shall inform and apply for approval from the Authority prior to engaging in their proposed role.

- R2-2.4.6 The Licence Holder shall ensure that proposed persons submit to the Authority, as part of the fitness and properness assessment on the proposed person, the Personal Questionnaire and any forms which may be requested. The Authority shall initiate the fitness and properness assessment upon submission of the complete form and supporting documentation as stipulated therein.

Such assessment will be undertaken in line with the [Guidance on the fitness and properness assessment applied by the Authority](#), as updated from time to time, which shall include an assessment of the following criteria:

- i. competence;
- ii. reputation;
- iii. conflicts of interest; and
- iv. time commitment, where applicable.

- R2-2.4.7 The Licence Holder or the proposed person. may also be required to provide further information. For the purposes of this rule, the MFSA may *inter alia* conduct interviews and request any supporting documentation it may deem necessary.

- R2-2.4.8 Where the proposed person is deemed to be fit and proper, the Authority shall issue its 'in-principle' approval in writing to the appointment or designation of the person within the Licence Holder.

Provided that the appointed person may also be required to fulfil certain conditions within set timeframes. These conditions shall be indicated in the approval letter.

Provided further that the appointed person may only commence their involvement with the Licence Holder upon satisfaction of the conditions set out in the approval letter.

The Departure Process

R2-2.4.9 The Licence Holder shall notify the Authority of the resignation or removal of any Appointed Person by not later than five working days from the date of notice of resignation. The Licence Holder shall also provide to the Authority together with this notification, a written statement noting the reason/s for departure and the remedial measures being taken to satisfy the licensing conditions as applicable. The notification should be submitted to the Authority through the chat box function of the [LH Portal](#). Any documentation requested in writing should be submitted to the Authority in original.

R2-2.4.10 The Licence Holder shall request the person referred to in R2-2.4.9, to provide to the Authority:

- i. the reason for their departure; and
- ii. a written confirmation that such departure was not a consequence of any regulatory implications or to provide relevant details of any such regulatory implications, as appropriate; and

Provided that the person referred to in R2-2.4.9 may be requested to attend an exit interview.

R2-2.5 Requirements Relating to Sound & Prudent Management

General Governance Arrangements

R2-2.5.1 In complying with the rules in this section, Licence Holders shall be guided by the following guidelines & publications as may be amended from time to time:

- i. the MFSA's [Corporate Governance Code](#), as may be amended from time to time;

R2-2.5.2 The Licence Holder's business shall be effectively directed from Malta by at least two individuals in their role as either an Executive Director and/or Senior Management.

Provided that the Licence Holder may be required by the MFSA that the business shall be effectively directed by a larger number of individuals from Malta depending on the nature, scale and complexity of the business.

R2-2.5.3 The directors and other key function holders shall be of sufficiently good repute, possess sufficient knowledge and experience, commit sufficient time to perform their functions and be sufficiently experienced so as to ensure the sound and prudent management of the Licence Holder on an ongoing basis.

R2-2.5.4 The Licence Holder shall take reasonable steps to ensure continuity and regularity in the performance of its activities. To this end, the Licence Holder shall employ appropriate and proportionate systems, resources and procedures.

R2-2.5.5 The Licence Holder shall:

- i. ensure that its personnel are aware of the procedures which must be followed for the proper discharge of their responsibilities;
- ii. employ personnel with the skills, knowledge and expertise necessary for the discharge of responsibilities allocated to them;
- iii. maintain adequate and orderly records of its business and internal organisation;
- iv. ensure that the performance of multiple functions by its relevant persons does not, and is not likely to, prevent those persons from discharging any particular function soundly, honestly and professionally; and
- v. establish a code of conduct/ ethics framework which promotes an ethical and professional culture;
- vi. ensure that no individual has concentration of power or undue influence.

For these purposes, the Licence Holder shall take into account the nature, scale and complexity of its business, and the nature and range of activities undertaken in the course of that business.

R2-2.5.6 Without prejudice to R2-2.5.5, the Licence Holder shall establish, implement and maintain:

- i. an adequate and effective internal governance and internal control framework that includes a clear organisational structure and well-functioning independent internal audit and compliance functions that have sufficient authority, stature and resources to perform their functions and comply with the applicable regulatory framework;
- ii. effective procedures to identify, manage, monitor and report the risks to which it is or might be exposed, including operational and security risks relating to services which may be provided by the Licence Holder;
- iii. decision-making procedures and an organisational structure with well-defined, transparent and consistent lines of responsibility;
- iv. effective internal reporting and communication of information at all relevant levels of the Licence Holder;
- v. systems and procedures that are adequate to safeguard the security, integrity and confidentiality of information, taking into account the nature of the information in question;
- vi. adequate internal control mechanisms, including sound administrative and accounting procedures, designed to secure compliance with decisions and procedures at all levels of the Licence Holder including procedures that enable it to deliver in a timely manner to the MFSA upon request, financial reports which reflect a true and fair view of its financial position and which comply with all applicable accounting standards and rules;
- vii. sufficient records to be able to demonstrate compliance with the conditions of its Licence as required;
- viii. adequate business continuity arrangements in terms of R2-2.5.43. The business continuity arrangements shall be aimed at ensuring, in the case of an interruption to its systems and procedures, the preservation of essential data and functions and the maintenance of its services, or, where that is not possible, the timely recovery of such data and functions and the timely resumption of its services;
- ix. adequate security arrangements including *inter alia* in relation to cyber security; and
- x. sound security mechanisms in place to guarantee the security and authentication of the means of transfer of information, minimise

the risk of data corruption and unauthorised access and to prevent information leakage maintaining confidentiality of data at all times. For purposes of this Rule 'security' shall also include cyber security.

Responsibility of the Board of Directors

R2-2.5.7 Licence Holders shall ensure that each member of its Board of Directors shall act with honesty, integrity, and independence of mind to effectively assess and challenge the decisions of the senior management where necessary and to effectively oversee and monitor management decision-making. The Licence Holder shall also ensure that the Board of Directors has collective independence from the group, where applicable.

R2-2.5.8 Without prejudice to R2-2.5.2 the Board of Directors shall:

- i. be composed of at least three (3) members;
- ii. include at least one (1) Independent Non-Executive Director;
- iii. have a balance of executive and non-executive directors; and
- iv. have at least one (1) member who is resident in Malta.

Provided that a larger number of directors and/or a different composition of executive directors, non-executive directors and independent non-executive directors may be required depending on the nature, scale and complexity of the Licence Holder's business and its shareholding structure.

R2-2.5.9 The Board of Directors of the Licence Holder shall be vested with the responsibility to abide by all requirements under the Act and any regulations made and rules issued thereunder.

R2-2.5.10 The Board of Directors shall meet regularly on at least a quarterly basis.

R2-2.5.11 The Chairperson of the board shall meet the following conditions:

- i. the Chairperson of the Board of Directors shall be an independent non-executive member.
- ii. 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.
- iii. the Chairperson shall set meeting agendas and ensure that strategic issues are discussed with priority.
- iv. 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.

Provided that a temporary derogation from the requirement set out in R2-2.5.11(i) may be provided. Any such derogation will be provided in writing following a reasonably justified request by a Licence Holder.

- R2-2.5.12 The Licence Holder shall:
- i. ensure board packs are circulated in good time prior to board meetings;
 - ii. retain adequate records of board meetings, including board packs and duly approved board minutes which are well documented and allow the reader to understand the rationale underlying any decisions taken, including any specific concerns raised by Directors;
 - iii. ensure that unapproved individuals do not participate in board meetings on a regular basis . Attendance by any such individuals shall be permitted only on an exceptional basis and with the prior consent of the Chairperson, solely for specific agenda items where their input is required.
- R2-2.5.13 Directors sitting on the Board shall constructively challenge and critically review propositions, explanations and information received when exercising judgement and taking decisions.
- R2-2.5.14 Licence Holders shall ensure that the Board of Directors define, approve and oversee:
- i. the overall business strategy and key policies of the Licence Holder taking into account the Licence Holder's long-term financial interest and solvency;
 - ii. adequate and effective internal governance and internal control framework that 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;
 - iii. the organisation of the Licence Holder for the provision of services and/or activities, including the skills, knowledge and expertise required by personnel, including key function holders, the resources, the procedures and the arrangements for the provision of services, taking into account the nature, scale and complexity of its business and all the requirements the firm has to comply with;

- iv. the implementation of the governance arrangements that ensure sound and prudent management of the Licence Holder, including the segregation of duties in the organisation and the prevention of conflicts of interest;
- v. targets for the liquidity management of the Licence Holder;
- vi. arrangements aimed at ensuring the internal functioning of each committee of the Board of Directors, when established, detailing the:
 - a. role, composition and tasks of each of them;
 - b. 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;
- vii. a conflict of interest policy at institutional level in line with R2-2.5.21;
- viii. formal and transparent procedures for the determination of the remuneration of the directors and executive staff in line with R2-2.5.24;
- ix. procedures for the regular assessment and evaluation of the collective performance of the Board of Directors and its committees except for; and
- x. a selection and suitability assessment process for the Board of Directors, CEO and key function holders.
- xi. the process for the selection, appointment, re-appointment and succession planning of members of the management body and the applicable internal procedure for the assessment of the suitability of a member including the internal function responsible for providing support for the assessment.

R2-2.5.15

The Licence Holder shall ensure that:

- i. members of the Board of Directors have adequate access to information and documents which are needed to oversee and monitor management decision-making;
- ii. individuals responsible for internal control functions are able to act independently and raise concerns directly with the non-executive directors sitting on the board where necessary, when adverse risk developments affect or may affect the Licence Holder.

R2-2.5.16 The governance arrangements referred to in this section shall comply with the following principles:

- i. the Board of Directors shall have the overall responsibility of the Licence Holder and approve and oversee the implementation of the Licence Holder's strategic objectives, risk strategy, and internal governance;
- ii. the Board of Directors shall monitor and periodically assess the adequacy and implementation of the Licence Holder's strategic objectives in the provision of services, the effectiveness of the Licence Holder's governance arrangements and the adequacy of the policies relating to the provision of services to clients and take appropriate steps to address any deficiencies;
- iii. the Board of Directors shall assess whether and how material changes to the business or organisational structure of the Licence Holder may impact the soundness of the Licence Holder;
- iv. the Board of Directors shall ensure the integrity of the accounting and financial reporting systems, including financial and operational controls and compliance with the law and relevant standards;
- v. the Board of Directors shall oversee the process of disclosure and communications;
- vi. the Board of Directors shall be responsible for providing effective oversight of senior management;
- vii. the chairman of the Board of Directors of the Licence Holder shall not exercise simultaneously the functions of a chief executive officer within the same Licence Holder, unless justified by the Licence Holder and authorised by the MFSA;
- viii. where committees are established, these are composed of at least 3 individuals, including an independent non-executive director;
- ix. the Board of Directors shall monitor and periodically assess the effectiveness of the Licence Holder's governance arrangements and take appropriate steps to address any deficiencies; and
- x. the Board of Directors shall ensure adequate systems and controls from an Information Technology point of view, including *inter alia* with respect to cyber-security.

Responsibility of Senior Management

- R2-2.5.17 When allocating functions internally, the Licence Holder shall ensure that senior management are responsible for ensuring that the Licence Holder complies with its obligations under these Rules.
- R2-2.5.18 In particular, senior management and where appropriate, the Board shall be required to assess and periodically review the effectiveness of the policies, arrangements and procedures put in place to comply with the obligations under these Rules and to take appropriate measures to address any deficiencies.

Conflicts of Interest

- R2-2.5.19 A Licence Holder shall establish, implement and maintain effective organisational and administrative arrangements to identify, manage and prevent conflicts of interest as set out in this section. Such arrangements shall be appropriate to the size and organisation of the Licence Holder and the nature, scale and complexity of its business, to prevent conflicts of interest from adversely affecting the interests of its clients.
- R2-2.5.20 Licence Holders shall adopt appropriate and transparent reporting lines within its organisation in order to ensure that issues involving risks of non-compliance with conflicts of interest rules are given the necessary priority.
- R2-2.5.21 A Licence Holder shall establish a conflicts of interest policy which shall include the following:
- i. The identification of, with reference to the specific distribution activities, specific services, activities and ancillary services carried out by or on behalf of the Licence Holder, the circumstances which constitute or may give rise to a conflict of interest entailing a risk of damage to the interests of one or more clients; and
 - ii. Procedures to be followed and measures to be adopted in order to manage such conflicts and to prevent such conflicts from damaging the interests of clients.
- R2-2.5.22 The Licence Holder shall assess and periodically review the conflict of interest policy established in accordance with these Rules and shall take all appropriate measures to address any deficiencies.

R2-2.5.23 The circumstances which should be treated as giving rise to a conflict of interest should cover cases where there is a conflict between the interests of the Licence Holder or certain persons connected to the Licence Holder including employees, or the group of which the Licence Holder forms part, or from the performance of services and activities, and the duty the Licence Holder owes to a client; or between the differing interests of two or more of its clients, to whom the Licence Holder owes in each case a duty.

At least the following situations that could create actual or potential conflicts of interest should be considered:

- i. economic interests (including shares, other ownership rights and memberships, holdings and other economic interests in commercial customers, intellectual property rights, loans granted by the institution to a company owned by members of the Board of Directors);
- ii. personal or professional relationships with the owners of qualifying holdings in the Licence Holder;
- iii. personal or professional relationships with the staff of the Licence Holder or related entities;
- iv. other employments and previous employments within the recent past (ex. 5 years);
- v. personal or professional relationships with relevant external stakeholders;
- vi. membership in a body or ownership of a body or entity with conflicting interested;
- vii. political influence or political relationships.

Remuneration Policy

R2-2.5.24 A Licence Holder shall define and implement remuneration policies and practices under appropriate internal procedures taking into account the interests of all its clients. The remuneration policy should be periodically reviewed.

R2-2.5.25 In defining its remuneration policies, a Licence Holder shall ensure that:

- i. clients are treated fairly and their interests are not impaired by the remuneration practices adopted by the Licence Holder in the short, medium or long term; and
- ii. remuneration policies and practices do not create a conflict of interest or incentive that may lead relevant persons to favour their own interests or the Licence Holder's interest to the potential detriment of its clients.

R2-2.5.26 The Licence Holder's Board of Directors shall approve the remuneration policy, after taking advice from the compliance function. Senior management of the Licence Holder shall be responsible for the day-to-day implementation of the remuneration policy and the monitoring of compliance risks related to the said policy.

Risk Consideration

R2-2.5.27 The Board of Directors shall approve and periodically review the strategies and policies for taking up, managing, monitoring and mitigating the risks the Licence Holder 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.

R2-2.5.28 The Board of Directors shall devote sufficient time to 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. The Licence Holder shall establish reporting lines to the Board of Directors that cover all material risks and risk management policies and changes thereof.

R2-2.5.29 The Board of Directors and, where a risk committee has been established, the Risk Committee shall have adequate access to information on the risk situation of the Licence Holder and, if necessary and appropriate, to the risk management function and to external expert advice.

R2-2.5.30 The Board of Directors in its supervisory function 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.

R2-2.5.31 The Licence Holder shall have in place adequate risk management processes and internal control mechanisms, including sound reporting and accounting procedures in order to identify, measure, monitor and control transactions with companies within their group appropriately. The Licence Holder shall report to the MFSA any significant transactions with those entities.

Compliance

R2-2.5.32 The Licence Holder shall establish, implement and maintain adequate policies and procedures designed to detect any risk of failure by the Licence Holder to comply with its obligations under the Act, the Regulations issued thereunder and these Rules, as well as with its obligations under other applicable legislation, as well as to detect the associated risks, and shall put in place adequate measures and procedures designed to minimize such risk and to enable the MFSA to exercise its powers effectively.

The Licence Holder shall, for this purpose, take into account the nature, scale and complexity of its business and the nature and range of services undertaken in the course of that business.

R2-2.5.33 The Licence Holder shall establish and maintain a permanent and effective compliance function which operates independently, and which has the following responsibilities:

- i. to monitor and, on a regular basis, to assess the adequacy and effectiveness of the measures and procedures put in place in accordance with the requirements of R2-2.5.32, and the actions taken to address any deficiencies in the Licence Holder's compliance with its obligations;
- ii. to draw up and implement a compliance monitoring plan;
- iii. to advise and assist the relevant persons responsible for carrying out services to comply with the Licence Holder's legal and regulatory obligations, and
- iv. providing prompt feedback to the Authority with respect to any enquiries raised by the Authority

R2-2.5.34 In order to enable the compliance function to discharge its responsibilities properly, the Licence Holder shall ensure that the following conditions are satisfied:

- i. the compliance function shall have the necessary authority, resources, expertise and access to all relevant information;
- ii. a Compliance Officer shall be appointed and shall be responsible for the compliance function and for any reporting as to compliance required by these Rules;

- iii. the relevant persons involved in the compliance function shall not be involved in the performance of services or activities which they monitor; and
- iv. the method of determining the remuneration of the relevant persons involved in the compliance function shall not compromise their objectivity and shall not be likely to do so.

Annual Compliance Report

- R2-2.5.35 The Licence Holder shall submit to the MFSA on an annual basis, together with the annual audited financial statements pursuant to R2-2.8.2, a Compliance Report drawn up by its Compliance Officer in line with the guidance notes, which shall include:
- i. the Compliance Officer's Annual Compliance Monitoring Plan as approved by the Board of Directors and the outcome of such plan; and
 - ii. a list of regulatory breaches identified and their status.

- R2-2.5.36 The Licence Holder shall ensure that the Compliance Report is signed by at least one Director and may be countersigned by the Compliance Officer.

Money Laundering Reporting Officer

- R2-2.5.37 The Licence Holder shall appoint and have at all times in place an MLRO. The role of the MLRO is an onerous one and the Licence Holder shall ensure that it is only accepted by individuals who fully understand the extent of responsibilities attached to the role.
- R2-2.5.38 When appointing an MLRO, the Licence Holder shall ensure compliance with the applicable provisions of Part I of the [Implementing Procedures](#) as well as any sector-specific Implementing Procedures issued by the FIAU in terms of the provisions of the Prevention of Money Laundering and Funding of Terrorism Regulations.

Internal Audit

- R2-2.5.39 The Licence Holder shall establish and maintain an internal audit function which is separate and independent from the other functions and activities of the Licence Holder and which has the following responsibilities:

- i. to establish, implement and maintain an audit plan to examine and evaluate the adequacy and effectiveness of the Licence Holder's systems, internal control mechanisms and arrangements;
- ii. to issue recommendations based on the result of work carried out in accordance with point (i) of this Rule;
- iii. to verify compliance with those recommendations; and
- iv. to report in relation to internal audit matters.

R2-2.5.40 The internal audit function shall, in particular, assess:

- i. the appropriateness of the Licence Holder's governance framework;
- ii. whether existing policies and procedures remain adequate and comply with legal and regulatory requirements;
- iii. whether procedures are correctly and effectively implemented; and
- iv. the adequacy, quality and effectiveness of the controls performed and reporting undertaken by other internal control functions.

R2-2.5.41 The Authority may provide a temporary derogation from the requirement for the internal audit function to be separate and independent as set out in R2-2.5.39. Any such derogation will be provided in writing following a reasonable justified request by a Licence Holder.

R2-2.5.42 Where the Licence Holder outsources the internal audit function, the Licence Holder shall appoint a director who shall be responsible for the oversight of this function.

Business Continuity Arrangements

R2-2.5.43 The Licence Holder shall establish business continuity arrangements which shall include a clear identification of the critical operations, effective and well-documented contingency, business continuity and recovery plans and a procedure to regularly review the adequacy of such plans.

R2-2.5.44 The business continuity management shall consist of:

- i. a Business Impact Analysis ('BIA')
- ii. a Business Continuity Plan ('BCP');
- iii. a Disaster Recovery Plan ('DRP');

- R2-2.5.45 The BIA shall include an analysis of the Licence Holder's exposure to severe business disruptions and assess their potential impacts (including on confidentiality, integrity and availability) quantitatively and qualitatively, using internal and/or external data (e.g. third party provider data relevant to a business process or publicly available data that may be relevant to the BIA) and scenario analysis. The BIA should also consider the criticality of the identified and classified business functions, supporting processes, third parties and information assets, and their interdependencies.
- R2-2.5.46 The BCP shall be based on the BIA and shall specifically consider the risks that could adversely impact the Licence Holder's systems and ensure that the Licence Holder is able to react appropriately to potential failures scenarios and recover the operations of its critical business activities after disruptions.
- R2-2.5.47 The DRP shall define the resources (hardware, software, communications, data as well as human resources), actions and tasks required to ensure the availability, continuity and recovery of the infrastructure needed to support the Licence Holder's business functions. This document may form part of the BCP.
- R2-2.5.48 The Licence Holder shall test its BCP and DRP on an annual basis and update the BCP and DRP based on testing results, current threat intelligence and lessons learned from previous events.

R2-2.6 Outsourcing Requirements

General

- R2-2.6.1 Pursuant to Article 8B(3) of the Act, the rules below outline the general principles regulating the conduct of outsourcing of functions undertaken by Licence Holders, which includes the outsourcing of important operational functions including IT systems.
- R2-2.6.2 Licence Holders shall, when complying with the Outsourcing Requirements, have regard to the principle of proportionality. Licence Holders are to apply these Requirements in a manner that is appropriate, taking into account, in particular:
- i. their size and internal organisation; the nature, scope and complexity of their activities; the complexity of the outsourced functions;
 - ii. the risks arising from the outsourcing arrangement;

- iii. the criticality or importance of the outsourced function; and
- iv. the potential impact of the outsourcing on the continuity of their activities.

R2-2.6.3 It is acknowledged that Licence Holders while undertaking their business activities may enter into outsourcing arrangements with third parties in order to be able to provide their services. Where:

- i. the Authority identifies concerns that lead to the conclusion that a Licence Holder no longer has robust governance arrangements in place; or
- ii. does not comply with regulatory requirements, including with regards to these rules established under this section in relation to outsourcing arrangements, or
- iii. the outsourcing arrangement hinders the Authority's ability to effectively supervise the Licence Holder;

Appropriate measures may be taken, including but not limited to, limiting or restricting the scope of the outsourced functions or requiring the Licence Holder to exit from an outsourcing arrangement and, or if necessary, for the outsourcing arrangement to be cancelled.

Assessment of What Constitutes Outsourcing

R2-2.6.4 The Licence Holder shall, on an ongoing basis, establish which of its arrangements with third parties fall under the definition of outsourcing as defined under the Act.

R2-2.6.5 Pursuant to R2-2.6.4, in assessing which of the arrangements with third parties fall under the definition of outsourcing as defined under the Act, the Licence Holder shall give due consideration to:

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

R2-2.6.6 The Licence Holder shall on an ongoing basis also identify which of their outsourcing arrangements are deemed to be critical or important.

Critical or Important Functions

R2-2.6.7 Pursuant to R2-2.6.6 the Licence Holder shall always consider a function as critical or important in the following situations:

- a) where a defect or failure in its performance would materially impair:
 - a. the Licence Holder's continuing compliance with the conditions of its authorisation or other obligations under the Financial Institutions Act and, or the Regulations and, or the Rules issued thereunder, and the Licence Holder's regulatory obligations;
 - b. the Licence Holder's financial performance; or
 - c. the Licence Holder's soundness;
- b) when operational tasks of internal control functions are outsourced, unless the assessment establishes that a failure to provide the outsourced function or the inappropriate provision of the outsourced function would not have an adverse impact on the effectiveness and quality of the internal control function;
- c) when they intend to outsource functions of payment and, or electronic money services to an extent that would require authorisation by a competent authority in a Member State or in a third country.

R2-2.6.8 When assessing whether an outsourcing arrangement relates to a function that is critical or important, the Licence Holder shall take into account at least the following factors:

- a) whether the outsourcing arrangement is directly connected to the provision of payment and, or electronic money services for which they are authorised;
- b) the potential impact of any disruption to the outsourced function or failure of the service provider to provide the service at the agreed service levels on a continuous basis on their:
 - i. short and long-term financial resilience and viability, including, if applicable, its assets, capital, costs, funding, liquidity, profits and losses;
 - ii. business continuity and operational resilience;
 - iii. operational risk, including conduct, information and communication technology (ICT) and legal risks;
 - iv. reputational risks;

- c) the potential impact of the outsourcing arrangement on their ability to:
 - i. identify, monitor and manage all risks;
 - ii. comply with all legal and regulatory requirements;
 - iii. conduct appropriate audits regarding the outsourced function;
- d) the potential impact on the services provided to its clients;
- e) all outsourcing arrangements, the Licence Holder's aggregated exposure to the same service provider and the potential cumulative impact of outsourcing arrangements in the same business area;
- f) the size and complexity of any business area affected;
- g) the possibility that the proposed outsourcing arrangement might be scaled up without replacing or revising the underlying agreement;
- h) the ability to transfer the proposed outsourcing arrangement to another service provider, if necessary or desirable, both contractually and in practice, including the estimated risks, impediments to business continuity, costs and time frame for doing so ('substitutability');
- i) the ability to reintegrate the outsourced function into the Licence Holder, if necessary or desirable;
- j) the protection of data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity on the Licence Holder and its clients, including but not limited to compliance with Regulation (EU) 2016/679 (GDPR);
- k) the outcome of the risk assessment undertaken in terms of R2-2.6.2.

Notification Requirements in respect of Outsourcing of Operational Functions relating to the provision of services listed in the First Schedule of the Act with the exception of activity 4 and/or 10.

R2-2.6.9 The Licence Holder shall, prior to outsourcing any operational function relating to the provision of services listed the First Schedule of the Act with the exception of activity 4 and/or 10, provide the Authority with the following information:

- i. the name, registered address and relevant contact details of the outsourcing service provider; and
- ii. a description of the operational function to be outsourced;
- iii. a confirmation that the outsourced function is not critical or important;

Provided that further information may be requested.

R2-2.6.10 Where a Licence Holder intends to outsource a critical or important operational function relating to the provision of services listed in the First Schedule of the Act with the exception of activity 4 and/or 10, it shall submit an FI Outsourcing Notification Form to the MFSA through the LH Portal at least 60 calendar days prior to entering into such outsourcing.

The FI Outsourcing Notification Form may be downloaded from <https://www.mfsa.mt/our-work/financial-institutions/>.

R2-2.6.11 The Licence Holder shall notify the Authority of any changes to any of the information notified pursuant to R2-2.6.9 and R2-2.6.10 without undue delay and shall make available on request all information necessary to enable the Authority to effectively supervise the compliance of the Licence Holder with the Outsourcing Requirements as established under these rules.

Provided that where changes relate to the outsourcing of important or critical functions, the Licence Holder shall submit an updated FI Outsourcing Notification Form clearly indicating the updated information.

R2-2.6.11.1 Without prejudice to R2-2.6.3, the Authority shall not require prior approval of outsourcing notifications submitted by Licence Holders.

Sound Governance Arrangements and Outsourcing

R2-2.6.12 Outsourcing shall not result in the delegation by the senior management of its responsibility. Within this context, the Board of Directors of the Licence Holder shall at all times remain fully responsible and accountable for at least:

- i. ensuring that the Licence Holder meets on an ongoing basis the conditions with which it must comply to remain authorised, including any conditions which may be imposed by the Authority;

- ii. the internal organisation of the Licence Holder;
- iii. the identification, assessment and management of conflicts of interest;
- iv. the setting of the Licence Holder's strategies and policies (e.g. the business model, the risk appetite, the risk management framework)
- v. overseeing day-to-day management of the Licence Holder including the management of all risks associated with outsourcing; and
- vi. the oversight role of Non-Executive Directors, including overseeing and monitoring management decision-making.

R2-2.6.13 Outsourcing shall not lower the suitability requirements applied to the members of the Board of Directors and key function holders. The Licence Holder shall have adequate competence and sufficient and appropriately skilled resources to ensure appropriate management and oversight of the outsourcing arrangements.

R2-2.6.14 The Licence Holder shall:

- i. clearly assign the responsibilities for the documentation, management and control of outsourcing arrangements;
- ii. allocate sufficient resources to ensure the documentation and monitoring of all outsourcing arrangements;
- iii. designate a key function holder or an Executive Director who shall be responsible for managing and overseeing the risks of outsourcing arrangements as part of the Licence Holder's internal control framework and overseeing the documentation of outsourcing arrangements and who shall report and be directly accountable to the Board of Directors;
- iv. maintain at all times sufficient substance and not become 'empty shells' or 'letter-box entities' and to this end the Licence Holder shall:
 - a. meet all the conditions of its authorisation at all times, including the Board of Directors effectively carrying out their responsibilities as set out in this Chapter;

- b. retain a clear and transparent organisational framework and structure that enables it to ensure compliance with legal and regulatory requirements;
 - c. where operational tasks of internal control functions are outsourced, exercise appropriate oversight and be able to manage the risks that are generated by the outsourcing of critical or important functions; and
 - d. have sufficient resources and capacities to ensure compliance with points (a) to (c).
- v. ensure that it can take and implement decisions related to its business activities and critical or important functions, including with regard to those that have been outsourced;
- vi. ensure that it maintains the orderliness of the conduct of its business and the regulated activities it undertakes;
- vii. ensure that the risks related to current and planned outsourcing arrangements are adequately identified, assessed, managed and mitigated, including risks related to ICT and financial technology;
- viii. ensure appropriate confidentiality arrangements are in place regarding data and other information;
- ix. ensure that an appropriate flow of relevant information with service providers is maintained; and
- x. ensure that where personal data is processed by outsourcing service providers, appropriate measures are implemented, and data is processed in accordance with Regulation (EU) 2016/679 (GDPR).

R2-2.6.15 The Licence Holder shall ensure that when outsourcing important or critical functions, it is able to undertake at least one of the following actions within an appropriate time frame:

- i. transfer the function to alternative service providers;
- ii. reintegrate the function; or
- iii. discontinue the business activities that are dependent on that function.

Outsourcing Policy

R2-2.6.16 The Licence Holder shall approve and regularly review and update an outsourcing policy.

R2-2.6.17 The outsourcing policy shall:

- i. consider the impact of outsourcing on the Licence Holder's business and the risks it faces;
- ii. define the principles, responsibilities and processes in relation to outsourcing;
- iii. include the reporting and monitoring arrangements to be implemented throughout the life-cycle of outsourcing arrangements, including contractual stages and exit stages;
- iv. ensure that outsourcing arrangements do not hinder effective on-site or off-site supervision of the Licence Holder; and
- v. also cover intra-group outsourcing arrangements and take into account any specific group circumstances.

R2-2.6.18 The outsourcing policy shall cover at least:

- i. the responsibility of the Board of Directors pursuant to R2-2.6.12, including its involvement, as appropriate, in the decision-making on outsourcing of critical or important functions;
- ii. the involvement of business lines, internal control functions and other individuals in respect of outsourcing arrangements;
- iii. the planning of outsourcing arrangements, including:
 - a. the definition of business requirements regarding outsourcing arrangements;
 - b. the criteria and process for identifying critical or important functions pursuant to R2-2.6.6 and R2-2.6.7;
 - c. risk identification, assessment and management vis-à-vis outsourcing arrangements;
 - d. due diligence checks on prospective outsourcing service providers;

- e. procedures for the identification, assessment, management and mitigation of potential conflicts of interest;
 - f. business continuity planning; and
 - g. the approval process of new outsourcing arrangements.
- iv. the implementation, monitoring and management of outsourcing arrangements, including:
 - a. the ongoing assessment of the outsourcing service provider's performance;
 - b. the procedure for being notified and responding to changes to an outsourcing arrangement or service provider;
 - c. the independent review and audit of compliance with legal and regulatory requirements; and
 - d. the renewal process;
- v. the documentation and record-keeping relating to outsourcing arrangements; and
- vi. the exit strategies and termination processes, including a requirement for a documented exit plan for critical or important function to be outsourced where such an exit is considered possible taking into account possible service interruptions or unexpected termination of an outsourcing agreement.

R2-2.6.19 Pursuant to R2-2.6.17, the outsourcing policy shall differentiate between the following:

- i. outsourcing of critical or important functions and other outsourcing arrangements;
- ii. outsourcing to service providers that are authorised to provide financial services in the EU and those that are not;
- iii. intragroup outsourcing arrangements and outsourcing to entities outside the group; and
- iv. outsourcing to service providers located in the EU and those located in third countries.

R2-2.6.20 The Licence Holder shall ensure that the outsourcing policy covers the identification of the following potential effects of critical or important

outsourcing arrangements and that these are taken into account in the decision-making process:

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

Conflicts of Interest

- R2-2.6.21 The Licence Holder shall identify, assess, and manage conflicts of interests in relation to its outsourcing arrangements and where the outsourcing arrangements create material conflicts of interest, including between entities within the same group, the Licence Holder shall take appropriate measures to manage those conflicts of interest.

Business Continuity Plans

- R2-2.6.22 The Licence Holder shall have in place, maintain and periodically test appropriate business continuity plans with regards to outsourced critical or important functions.

Internal Audit Function

- R2-2.6.23 The Licence Holder's internal audit function activities shall cover, following a risk-based approach, the independent review of outsourced activities. The audit plan and programme should include, in particular, the outsourcing arrangements of critical or important functions.
- R2-2.6.24 With regard to the outsourcing process, the Licence Holder's internal audit function should at least ascertain:
- a. that the Licence Holder's framework for outsourcing, including the outsourcing policy, is correctly and effectively implemented and is in line with the applicable laws and regulation, the risk strategy and the decisions of the Board of Directors;
 - b. the adequacy, quality and effectiveness of the assessment of the criticality or importance of functions;
 - c. the adequacy, quality and effectiveness of the risk assessment for outsourcing arrangements and that the risks remain in line with the Licence Holder's risk strategy;
 - d. the appropriate involvement of governance bodies; and

- e. the appropriate monitoring and management of outsourcing arrangements.

Documentation Requirements

- R2-2.6.25 The Licence Holder shall establish and maintain a register of all of the Licence Holder's current outsourcing arrangements, distinguishing between the outsourcing of critical or important functions and other outsourcing arrangements.

The Licence Holder shall consult the EBA Guidelines on Outsourcing for the purposes of this register.

- R2-2.6.26 The MFSA may require the Licence Holder to specify further information within the outsourcing register taking into account the criticality and importance of outsourced functions.

- R2-2.6.27 The Licence Holder shall, upon request, make available to the Authority either the full register of all existing outsourcing arrangements or sections specified thereof as determined by the Authority.

- R2-2.6.28 The Licence Holder shall, upon request, make available to the Authority all information necessary, including a copy of the outsourcing agreement, to enable the Authority to execute the effective supervision of the Licence Holder.

- R2-2.6.29 The Licence Holder shall refer to the provisions on '*Documentation Requirements*' as explained in the [EBA Guidelines on Outsourcing](#), as may be amended from time to time, and shall ensure compliance therewith.

The Outsourcing Process

Pre-outsourcing analysis

- R2-2.6.30 Prior to entering into any outsourcing arrangement, the Licence Holder shall:
- i. assess if the outsourcing arrangement concerns a critical or important function;
 - ii. ensure that where regulated activities are outsourced, the outsourcing service provider is duly authorised to undertake such regulated activities;

- iii. identify and assess all relevant risks of the outsourcing arrangement;
- iv. undertake appropriate due diligence on the prospective service provider; and
- v. identify and assess conflicts of interest that the outsourcing may cause.

Risk assessment of Outsourcing Arrangements

- R2-2.6.31 The Licence Holder shall assess the potential impact of outsourcing arrangements on their operational risk, shall take into account the assessment results when deciding if the function should be outsourced to a service provider and shall take appropriate steps to avoid undue additional operational risks before entering into outsourcing arrangements.

Due Diligence

- R2-2.6.32 Before entering into an outsourcing arrangement and considering the operational risks related to the function to be outsourced, the Licence Holder shall ensure in their selection and assessment process that the service provider is suitable.
- R2-2.6.33 With regards to critical and important functions, the Licence Holder shall ensure that the service provider has the business reputation, appropriate and sufficient abilities, the expertise, the capacity, the resources (e.g. human, IT, financial), the organisational structure and, if applicable, the required regulatory authorisation(s) or registration(s) to perform the critical or important function in a reliable and professional manner to meet its obligations over the duration of the draft contract.

Contractual Phase

- R2-2.6.34 The Licence Holder shall ensure that any outsourcing arrangement is based on a formal, clear, written agreement which establishes the respective rights and obligations of the Licence Holder and of the service provider.
- R2-2.6.35 The outsourcing agreement for critical or important functions shall set out at least:

- i. a clear description of the outsourced function to be provided;
- ii. the start date and end date, where applicable, of the agreement and the notice periods for the service provider and the Licence Holder;
- iii. the governing law of the agreement;
- iv. the parties' financial obligations;
- v. whether the sub-outsourcing of a critical or important function, or material parts thereof, is permitted and, if so, the conditions that the sub-outsourcing is subject to;
- vi. the location(s) (i.e. regions or countries) where the critical or important function will be provided and/or where relevant data will be kept and processed, including the possible storage location, and the conditions to be met, including a requirement to notify the Licence Holder if the service provider proposes to change the location(s);
- vii. where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data;
- viii. the right of the Licence Holder to monitor the service provider's performance on an ongoing basis;
- ix. the agreed service levels, which should include precise quantitative and qualitative performance targets for the outsourced function to allow for timely monitoring so that appropriate corrective action can be taken without undue delay if the agreed service levels are not met;
- x. the reporting obligations of the service provider to the Licence Holder, including the communication by the service provider of any development that may have a material impact on the service provider's ability to effectively carry out the critical or important function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements and, as appropriate, the obligations to submit reports of the internal audit function of the service provider;
- xi. whether the service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;

- xii. the requirements to implement and test business contingency plans;
- xiii. provisions that ensure that the data that are owned by the Licence Holder can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the service provider;
- xiv. the obligation of the service provider to cooperate with the MFSA, including other persons appointed by it;
- xv. the unrestricted right of Licence Holders and competent authorities to inspect and audit the service provider with regard to, in particular, the critical or important outsourced function; and
- xvi. termination rights.

Sub-Outsourcing of Critical or Important Functions

- R2-2.6.36 The Licence Holder shall ensure that the outsourcing agreement specifies whether or not sub-outsourcing of critical or important functions, or material parts thereof, is permitted.
- R2-2.6.37 Where sub-outsourcing of critical or important functions is permitted, the Licence Holder shall determine whether the part of the function to be sub-outsourced is, as such, critical or important (i.e. a material part of the critical or important function) and, if so, record it in the register.

Security of Data and Systems

- R2-2.6.38 The Licence Holder shall ensure that service providers, where relevant, comply with appropriate IT security standards.

Access, Information and Audit rights

- R2-2.6.39 The Licence Holder shall ensure within the written outsourcing arrangement that its internal audit function is able to review the outsourced function using a risk-based approach.

Regardless of the criticality or importance of the outsourced function, the written outsourcing arrangements between the Licence Holder and service providers shall refer to the information gathering and investigatory powers of the Authority with regard to service providers located in a Member State

and should also ensure those rights with regard to service providers located in third countries.

R2-2.6.40 With regard to the outsourcing of critical or important functions, the Licence Holder shall ensure within the written outsourcing arrangement that the service provider grants them and the Authority, and any other person appointed by them or by the Authority, the following:

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

Termination Rights

R2-2.6.41 The outsourcing arrangement shall expressly allow the possibility for the Licence Holder to terminate the arrangement in accordance with applicable law and the arrangement shall also facilitate the transfer of the outsourced function to another service provider or its re-incorporation into the Licence Holder.

Oversight of Outsourced Functions

R2-2.6.42 The Licence Holder shall monitor, on an ongoing basis, the performance of the service providers with regard to all outsourcing arrangements on a risk-based approach and with the main focus being on the outsourcing of critical or important functions, including that the availability, integrity and security of data and information is ensured. Where the risk, nature or scale of an outsourced function has materially changed, the Licence Holder should reassess the criticality or importance of that function.

The Licence Holder shall apply due skill, care and diligence when monitoring and managing outsourcing arrangements.

R2-2.6.43 The Licence Holder shall regularly update its risk assessment with respect to outsourcing arrangements and periodically report to the Board of

Directors on the risks identified in respect of the outsourcing of important or critical functions.

The Licence Holder shall monitor and manage its internal concentration risks caused by outsourcing arrangements as part of its risk assessment on outsourcing arrangements.

R2-2.6.44 The Licence Holder shall ensure, on an ongoing basis, that outsourcing arrangements, particularly relating to critical or important functions, meet appropriate performance and quality standards by:

- i. ensuring that they receive appropriate reports from outsourcing service providers;
- ii. evaluating the performance of outsourcing service providers; and
- iii. reviewing all other relevant information received from outsourcing service providers, including reports on business continuity and testing.

R2-2.6.45 The Licence Holder shall take appropriate measures if it identifies shortcomings in the provision of the outsourced function. In particular, the Licence Holder shall follow up on any indications that service providers may not be carrying out the outsourced critical or important function effectively or in compliance with applicable laws and regulatory requirements. If shortcomings are identified, the Licence Holder shall take appropriate corrective or remedial actions, which may include terminating the outsourcing agreement, with immediate effect, if necessary.

R2-2.7 Accounting and Statutory Audit Requirements

R2-2.7.1 The Licence Holder shall comply with the applicable provisions of the [Act](#) as found in Title Accounting, Statutory Audit and Auditors.

R2-2.8 Reporting Requirements

R2-2.8.1 The Licence Holder shall comply with the requirements set out in [Directive 5](#) Statistical Reporting Requirements of the Central Bank of Malta.

Annual Reporting Requirements

R2-2.8.2 The Licence Holder shall be required to submit to the MFSA, within four (4)

months of the accounting reference date, the soft copies of the following:

- i. the Audited Annual Fintech Return;
- ii. a copy of the audited annual financial statements or consolidated financial statements, as applicable, prepared in accordance with the Companies Act and generally accepted accounting principles and practice;
- iii. a copy of the Auditor's management letter;
- iv. a copy of the Auditor's report to the MFSA, as applicable, as specified in R2-2.8.8.
- v. an up-to-date organisational structure chart including the correct reporting lines and three lines of defence and the personnel based in Malta.
- vi. An independent assurance report containing:
 - I. an Auditor confirmation that the audit has been conducted in accordance with International Standards on Auditing;
 - II. whether proper accounting records have been kept, and adequate systems for their control have been maintained, as required by the MFSA, during the period covered by the Audited Annual FinTech Return.
 - III. all information and explanations necessary for the purpose of the audit have been obtained.

R2-2.8.3 Pursuant to point (ii) of R2-2.8.2, the Licence Holder shall also require its Auditor to prepare a management letter in accordance with International Standards on Auditing.

R2-2.8.4 Furthermore, pursuant to point (ii) of R2-2.8.2, the Licence Holder is required to include in the Directors' Report or by way of a separate confirmation signed by the Directors, as applicable under the generally accepted accounting principles and practices, a statement regarding breaches of the Rules or other regulatory requirements which occurred during the reporting period, and which were subject to an administrative penalty or other regulatory sanction.

R2-2.8.5 The Directors' Report or the confirmation signed by the Directors, as applicable, shall contain a summary of the breach/breaches committed and

regulatory sanction/s imposed, if any. Where there have been no breaches, it shall contain a statement to that effect.

R2-2.8.6 Pursuant to point (iii) of R2-2.8.2, the Licence Holder in receipt of a management letter from its Auditor which contains recommendations to remedy any weaknesses identified during the course of the audit, is required to submit to the MFSA by not later than four months from the end of the financial period to which the management letter relates, a statement setting out in detail the manner in which the Auditor's recommendations have been/ are being implemented. In the instance where the Licence Holder has not taken / is not taking any action in respect of any one or more recommendations in the Auditor's management letter, the reasons are to be included.

R2-2.8.7 Pursuant to point (iv) of R2-2.8.2, the Auditor must also include a confirmation that the audit has been conducted in accordance with International Standards on Auditing and whether, in the Auditor's opinion:

- i. the Annual Audited Fintech Return has been prepared in accordance with the MFSA's requirements as set out in the Guidelines to the Fintech Return and is consistent with the audited financial statements; and
- ii. proper accounting records have been kept, and adequate systems for their control have been maintained, as required by the MFSA, during the period covered by the Annual Fintech Return;
- iii. all information and explanations necessary for the purpose of the audit have been obtained.

R2-2.8.8 Where, in the Auditor's opinion, one or more of the requirements have not been met, the Auditor shall be required to include in his report a statement specifying the relevant requirements and the respects in which they have not been met. Where the Auditor is unable to form an opinion as to whether the requirements have been met, the Auditor shall be required to specify the relevant requirements and the reasons why he has been unable to form an opinion.

Annual Fintech Return

R2-2.8.9 Dual-licensed entities shall each year prepare and submit the soft copy of the automated Annual Fintech Return to the MFSA within one (1) month from the accounting reference date. The Annual Fintech Return must be

prepared in accordance with the MFSA's requirements as set out in the Guidelines to the Fintech Return.

- R2-2.8.10 Where the Annual Fintech Return has been submitted before the relevant audited annual financial statements have been produced, it shall be updated to reflect the information in the audited financial statements and submitted to the MFSA together with the audited annual financial statements.

Interim Fintech Returns

- R2-2.8.11 Dual-licensed entities shall prepare an Interim Fintech Return, at dates three, six and nine months after the accounting reference date. The first Interim Fintech Return should cover the three months immediately following the accounting reference date, the second Interim Fintech Return should cover the six months immediately following the accounting reference date and the third Interim Fintech Return should cover the nine months immediately following the accounting reference date. In the event of a change to the accounting reference date, the dates for the preparation of the Interim Fintech Returns shall be agreed with the MFSA. The Interim Fintech Return must be prepared in accordance with the MFSA's requirements as set out in the Guidelines to the Fintech Return.
- R2-2.8.12 The soft copy of the Interim Fintech Return shall be submitted to the MFSA within one (1) month from the date up to which it has been prepared.

R2-2.9 Record Keeping

- R2-2.9.1 The Licence Holder shall arrange for Records to be kept of all services and transactions undertaken by it which shall be sufficient to enable MFSA to monitor compliance with the requirements under these Rules, and in particular to ascertain that the Licence Holder has complied with all obligations with respect to clients or potential clients.

Provided that the requirements set out in this Section shall be without prejudice to:

- i. any other record keeping obligations that the Licence Holder may have in terms of any other law, rules or regulation; and
- ii. the right of any other authority, in terms of applicable law, to access the documents, data or information covered by this Section.

- R2-2.9.2 The records referred to in R2-2.9.1 shall be retained for a period of at least 5 years.
- R2-2.9.3 The Records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the MFSA and in such a form and manner that the following conditions are met:
- i. the MFSA must be able to access them readily in a legible format and to reconstitute each key stage of the processing of each transaction; and
 - ii. it must not be possible for the records otherwise to be manipulated or altered.
- R2-2.9.4 The Licence Holder shall ensure that its IT infrastructure ensures:
- i. the integrity and security of any data stored therein;
 - ii. availability, traceability and accessibility of data; and
 - iii. privacy and confidentiality.
- R2-2.9.5 The Licence Holder shall ensure that its IT infrastructure is located in Malta, and/or any other EEA member state.

R2-2.10 Liquidity

- R2.2.10.1 The Authority emphasises the need for all Licence Holders to maintain continuous liquidity to ensure that they have sufficient assets to cover their liabilities and to be able to meet their obligations as and when they fall due.

Licence Holders shall have policies and procedures in place to ensure continuous liquidity. Moreover, Licence Holders shall have adequate systems and controls in place to ensure that the policies and procedures set are followed.

The responsibility for ensuring the continuous liquidity of a Licence Holder rests with the Board of Directors and its senior management.

R2-2.11 ICT and Security Risk

- R2-2.11.1 Financial institutions shall, taking into account their size, nature, scale and complexity of the business ensure compliance with the [Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements](#).

R2-2.12 Arm's Length Principle

- R2-2.12.1 This Rule extending the applicability of the "arm's length" principle ('the principle') is being made pursuant to Article 10(1)(b) of the Act, which determines the applicability of the principle both in relation to the granting of credit facilities and to the extension of other services by financial institutions. Furthermore, the same paragraph (b) of Article 10(1) of the Act also provides for the measures that are to be taken by the Authority to ensure compliance by financial institutions with this provision and for sanctioning financial institutions in cases of non-compliance.
- R2-2.12.2 In order to prevent abuses arising in transactions with related parties and to control or where appropriate mitigate conflicts of interest, financial institutions shall enter into any transactions with related parties on an arm's length basis, shall adopt adequate procedures for such transactions, establish adequate monitoring systems, take appropriate steps to control or mitigate the risks and write off exposures to related parties in accordance with standard policies and processes.
- R2-2.12.3 In granting credit facilities and in extending other services, financial institutions shall have procedures to ensure that 'related parties' are not granted nor have outstanding credit facilities or other services under terms more favourable (e.g. in credit assessment, tenor, interest rates, fees, amortization schedules, requirement for collateral) than those applied to other persons.
- R2-2.12.4 Financial institutions shall apply the principle to the following additional related parties over and above those currently included in paragraph (b) of article 10(1) of the Act:
- qualifying and significant shareholders, auditors, or their respective close family members, whether jointly or severally, and to any commercial partnership in which such persons may have control;
 - officers and employees of the financial institution, including members of the Board of Directors, their direct and related interests, and their close family members; and
 - corresponding persons in affiliated companies.

The Authority may exercise discretion in applying this definition on a case-by-case basis.

- R2-2.12.5 The provisions of paragraph R2-2.12.4 above shall not apply in respect of credit facilities and other services granted by financial institutions to their officers and employees under preferential terms as laid down in their conditions of employment.
- R2-2.12.6 Financial institutions shall ensure that there are specific procedures in place to prevent persons, benefiting from credit facilities and/or other services, from being part of the preparation and the assessment leading to the decision of granting such facilities and/or the provision of the services.
- R2-2.12.7 Financial institutions shall ensure that transactions with related parties and the write-off of related-party exposures exceeding specified amounts, or otherwise posing special risks, are subject to prior approval by the financial institution's Board. Members of the Board of Directors with conflicts of interest are to be excluded from the approval process of granting and managing related party transactions.
- R2-2.12.8 Financial institutions shall ensure that adequate policies and processes are in place with regards to identifying individual exposures and transactions with related parties, as well as the total amount of exposures, and the monitoring and reporting on them through an independent credit review or audit process. Any exceptions to policies, processes and the limits shall be reported to the appropriate level of the financial institution's senior management and, if necessary, to the Board, for timely action. Senior management shall monitor related party transactions on an ongoing basis, and the Board shall be bound to provide oversight of these transactions.

R2-2.13 Third Party Exposure Threshold

- R2-2.13.1 In cognisance of the fact that in carrying out certain activities listed in the First Schedule to the Act, specifically Activities 1, 2, 3 and 6, a Licence Holder would be committing itself to exposures with third party clients, the Authority deems that such exposures should also be appropriately monitored and regulated. In this respect the Authority would condition a Licence Holder that undertakes such activities to the rules below.
- R2-2.13.2 Licence Holders are required to limit their exposures to third-party clients or group of connected third-party clients to a maximum of 40% of their level of own funds. This requirement applies exclusively to receivables from third-party clients, excluding exposures to group entities, and pertains only to receivables arising from the Licence Holder's licenced activities.
- R2-2.13.3 The exposure amount considered for compliance with the maximum threshold set above shall be based on the carrying value of the relevant receivables as reported in the Interim/Annual/Annual Audited FI Return

submitted to the Authority. The threshold shall be applied individually to each third-party client or group of connected third-party clients.

R2-2.14 Capital Requirements

Initial Capital Requirement

- R2-2.14.1 Financial institutions licenced to carry out the activities found under the First Schedule to the Act (with the exception of activities 4 and/or 10), neither the Rule nor the Act establish a minimum or a set level of initial capital requirements in view of the fact that the risk profiles of the different types of financial institutions that can be licenced under this Act may result in considerable variation in the level of capital required to be held against such risk(s). Therefore, the initial capital of an applicant institution will be set by the Authority on a case-by-case basis and will be commensurate with the level of risk pertaining to the number and type of activities proposed to be undertaken and as laid out in the business plan submitted by the prospective applicants.

Own Funds

- R2-2.14.2 Financial Institutions carrying out Activities 1, 2, 3 and 6 of the First Schedule to the Act shall be required to hold own funds amounting to the higher of:

- i) Initial Capital Requirement
- OR
- ii) 5% of Total Adjusted Assets

Where Total Assets is the total assets reported in the Financial Institution Return submitted to the Authority and Total Adjusted Assets is calculated as total assets less any assets deducted in the calculation of own funds as per Article 26 of Regulation (EU) 575/2013.

- R2-2.14.3 Financial Institutions carrying out Activities 5, 7, 8 and 9 of the First Schedule to the Act shall be required to hold own funds amounting to the higher of:

- i) Initial Capital Requirement
- OR
- ii) 25% of Adjusted Total Expenditure

Where Total Expenditure is the the total expenditure reported in the previous Annual Audited Financial Institution Return submitted to the Authority and

the Adjusted Total Expenditure is calculated as total expenditure less the following deductions:

- a) Staff bonuses and other remuneration, to the extent that those bonuses and that remuneration depend on the net profit of the Licence Holder in the relevant year.
- b) Employees', directors', and partners' shares in profits, to the extent that they are fully discretionary.
- c) Other appropriations of profits and other variable remuneration, to the extent that they are fully discretionary.
- d) Non-recurring expenses from non-ordinary activities

R2-2.14.4 Provided that the where the Licence Holder has not completed a full year's business at the date of calculation, the projected expenditure included in its forecasts for the first twelve months of business, as submitted in the application for authorisation and as approved by the Authority, shall be used.

R2-2.14.5 The Authority may require a Licence Holder to hold an amount of own funds up to 20% higher or lower than the amount indicated in R2-2.14.2 or R2-2.14.3 based on an evaluation by the Authority of the Licence Holder's risk-management processes, risk loss databases and internal control mechanisms.

R2-2.15 Credit Risk Management Framework

R2-2.15.1 The Licence Holder shall implement a robust credit risk management framework for managing credit risk that is appropriate to the nature, scale and complexity of the Licence Holder's business. The framework shall include:

- (a) a credit risk appetite statement;
- (b) a credit risk management strategy and policies and procedures for identifying, measuring, evaluating, monitoring, reporting and mitigating credit risk consistent with the approved risk appetite set by the Board;
- (c) clearly defined and documented roles, responsibilities and formal reporting structures to manage credit risk;
- (d) a designated credit risk management function;
- (e) a management information system that is adequate, both under normal circumstances and in periods of stress, to measure, assess and report on credit risk; and

- (f) an independent review process to ensure that the framework is effective to identify, measure, evaluate, monitor, report, and control or mitigate credit risk.

The Licence Holder's credit risk management strategy and the main policies and procedures shall be approved and regularly reviewed by the Board.

R2-2.16 Complaints Handling

- R2-2.16.1 Financial institutions shall put in place a 'complaints management policy'. This policy should be defined and endorsed by the senior management of the financial institution, who should also be responsible for its implementation and for monitoring compliance with it.
- R2-2.16.2 The 'complaints management policy' shall be set out clearly in writing and shall be made available to all relevant staff of the financial institution through an adequate internal channel.
- R2-2.16.3 Financial institutions shall either designate an individual from Senior management to handle complaints or shall have in place a 'complaints management function' which enables complaints to be investigated fairly and possible conflicts of interest to be identified and mitigated.
- R2-2.16.4 Financial institutions shall maintain a Register in which every complaint and the action taken in its regard is recorded. This Register shall contain, inter alia, the following information:
 - a) the subject of the complaint;
 - b) the date on which the complaint was received;
 - c) the date when the complaint was answered by the institution;
 - d) the date when the complaint was resolved;
 - e) the result or outcome of the complaints handling procedure and;
 - f) a detailed description of the product in question, as applicable, to which the complaint refers.

The Authority may at any time require the Register to be produced for its review. The documentation relating to the complaint shall be kept and archived in a secure manner for a reasonable period based on the nature of the complaint.

- R2-2.16.5 Financial institutions shall provide information on complaints and complaints-handling to the Authority, where applicable and, or as and when required. This data shall cover the number of complaints received, differentiated as appropriate or as indicated in any criteria that the Authority may from time to time establish.

R2-2.16.6 Financial institutions shall analyse, on an on-going basis, complaints-handling data, to ensure that they identify and address any recurring or systemic problems, and potential legal and operational risks by, for instance, carrying out the following:

- a) analysing the causes of individual complaints to identify root causes common to types of complaint;
- b) considering whether such root causes may also affect other processes or products, including those not directly complained of; and
- c) correcting, where reasonable to do so, such root causes.

R2-2.16.7 Financial institutions shall:

- a) On request, provide written information to the Authority regarding their complaints-handling process;
- b) Publish details of their complaints-handling process in an easily accessible manner (for example, in brochures, pamphlets, contractual documents or via the financial institution's website);
- c) Provide clear, accurate and up-to-date information about the complaints-handling process including:
 - (i) Details of how to make a complaint (for example, the type of information to be provided by the complainant, the identity and contact details of the person or department to whom the complaint should be directed); and
 - (ii) The process that will be followed when handling a complaint (for example, when the complaint will be acknowledged, an indication of handling timelines and the availability of an authority, an ombudsman or Alternative Dispute Resolutions forums including complaints with the Arbiter for Financial Services under the Arbiter for Financial Services Act (Chapter 555 of the Laws of Malta)).
- c) Provide clear information on the language in which the complaint may be submitted to the financial institution which languages shall at least include the English language.

- R2-2.16.8 Financial institutions shall, within 2 working days, acknowledge receipt in writing of any complaint.
- R2-2.16.9 Where a complaint is made orally, financial institutions shall make a summary of the complaint and request the complainant to confirm in writing the said summary.
- R2-2.16.10 Financial institutions shall seek to gather and investigate all relevant evidence and information regarding the complaint before taking a final decision.
- R2-2.16.11 When a financial institution acknowledges receipt of a complaint in accordance with R2-2.16.8 and R2-2.16-9, the financial institution concerned shall also provide the complainant in writing with confirmation of the following:
- a) That the financial institution shall investigate the complaint;
 - b) That the financial institution shall, on completion of the investigation and without unnecessary delay, inform the complainant, in writing, about the outcome of the investigation and describing its proposed course of action; and
 - c) That if the investigation is not completed within 15 working days from the date of receipt of the complaint, the financial institution shall inform the complainant of such fact before the end of this period.
- R2-2.16.12 Where the financial institution envisages that the investigation of a complaint will not be completed within 15 working days from receipt of the complaint, the financial institution shall immediately:
- a) Inform the complainant that the investigation will not be completed within 15 working days from the receipt of the complaint;
 - b) Inform the complainant about the reasons of the causes of the delay;
 - c) Provide an indication as to when the investigation is likely to be completed; and
 - d) Inform the complainant that, if the complainant is not satisfied with the progress of the investigation, the matter may be referred by the complainant to other Alternative Dispute Resolution forums including complaints with the Arbiter for Financial Services under the Arbiter for Financial Services Act (Chapter 555 of the Laws of Malta).

- R2-2.16.13 When providing a final decision that does not fully satisfy the complainant's demand, financial institutions are expected, to the extent possible, to include a thorough explanation of the financial institution's position on the complaint and that the complainant may refer to other Alternative Dispute Resolution forums including complaints with the Arbiter for Financial Services under the Arbiter for Financial Services Act (Chapter 555 of the Laws of Malta).
- R2-2.16.14 Any form of communication in terms of the paragraphs above shall be communicated to the complainant clearly in plain language which is easily understood and in writing.
- R2-2.16.15 Financial institutions shall ensure that, when handling complaints in terms of this Rule, they shall abide with any data protection laws including the Data Protection Act (Chapter 586 of the Laws of Malta) and any regulations issued thereunder, and with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) as amended from time to time.

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

Malta Financial Services Authority

Triq L-Imdina, Zone 1

Central Business District, Birkirkara, CBD 1010, Malta

communications@mfsa.mt

www.mfsa.mt