



ΕΠΙΤΡΟΠΗ
ΚΕΦΑΛΑΙΑΓΟΡΑΣ
ΚΥΠΡΟΥ

CYPRUS SECURITIES AND EXCHANGE COMMISSION

REGULATED ENTITIES RBS-F HANDBOOK

The CySEC's Risk Based Supervision Framework ('RBS-F')

CONTENTS

Chairwoman’s Statement	3
Introduction.....	4
An overview of the Framework.....	6
Entity stances and approach to supervision	12
How risk based supervision works in practice.....	14

CHAIRWOMAN'S STATEMENT

CySEC recognizes the importance of having in place a robust risk assessment framework that would allow it to further strengthen supervision, maximise market compliance and enhance investor protection.

This is why it has decided to add to its supervisory toolbox a comprehensive supervision framework based on risk management, the **Risk-Based Supervision Framework** ("RBS-F").

The RBS-F is a structured approach to assess risk and was designed to assist CySEC in setting its regulatory priorities and adjust the intensity of supervision, focusing where risks are greater.

Through its use, emphasis is placed on those entities which are of greatest importance in terms of the risks they tend to have and their potential impact in case of failure, ensuring the smooth and stable operation of the securities market.

At the same time, it upgrades CySEC's ability to assess and analyse the particular characteristics of the regulated entities, so that it can swiftly address any challenges that affect both the entities and the security market as a whole.

Consequently, CySEC's judgment of the risk, significance and impact that each regulated entity poses to its statutory objectives will determine the overall intensity of the regulatory approach to be followed.

This risk-based approach is being considered the best and most widely used practice among Supervisory Authorities and it is in line with the regulatory practices adopted in Europe.

Overall, we strongly believe that the implementation of the RBS-F in the Cyprus securities market is an important milestone that greatly enhances investor protection and confidence, which is a prerequisite for the healthy development of the financial market and the economy at large.

Demetra Kalogerou

Chairwoman



INTRODUCTION

What is covered in this paper?

This document explains the key principles of the risk supervisory framework and aims to provide regulated entities with a general understanding of the rationale and practices to be followed by CySEC.

It sets out what regulated entities can expect from the risk assessment process and during their on-going supervisory cycle. Aim is to provide an understanding of the different approaches that will be followed by CySEC, depending on the profile of each entity.

Regulated entities will need to work closely with CySEC, so that to ensure that progress made to minimize risk is achieved.

Specifically, this paper explains:

- The framework, how risk is assessed and how this is linked to our objectives.
- How the framework is applied to our supervisory activities.
- What will the RBS-F mean for your firm.

Who should read this paper?

The RBS-F is implemented and is expected to have an effect on all entities regulated by CySEC, including:

- Cyprus Investment Firm (CIFs) – i.e. entities authorised under Law L144(I)/2007 as amended.
- Administrative Service Providers (ASPs) – i.e. entities under Law L196(I)/2012.
- Management Companies – i.e. fund managers (as these are defined in the Alternative Investments Fund Managers Law of 2013 (L56(I)/2013) and the UCI Law of 2012 (L 78(I)/2012) Section 2)) as

well as Self-Managed Funds (as these are defined in L56(I)/2013 Section 5(1)(b) and Law 131(I)/2014 Section 6(2)(a)) and Self Managed Funds with Limited Number of persons (as these defined in L56(I)/2013 Section 116(3)(a)).

Any of the above types of entities, which have been granted an authorisation from CySEC, will be subject to our risk based approach and will fall under the annual risk assessment process. Depending on the risk profile of the entity, the regulatory approach will differ.

The Management persons involved in the regulated entities' Controls, Functions and other relevant persons and stakeholders of regulated entities may want to have an understanding of the approach to be followed during our supervisory activities. Purpose of this document, is to provide such information.

The benefits from the RBS-F

The implementation of a risk based approach has a number of benefits both for CySEC, as well as for regulated entities.

The RBS-F, aims to assist CySEC control the risk of failing to meet its statutory obligations, while at the same time taking into consideration any reputational risk arising from its duties and its role within the international financial markets and that of the European Union (EU) specifically.

It is expected that CySEC, will be in a position to:

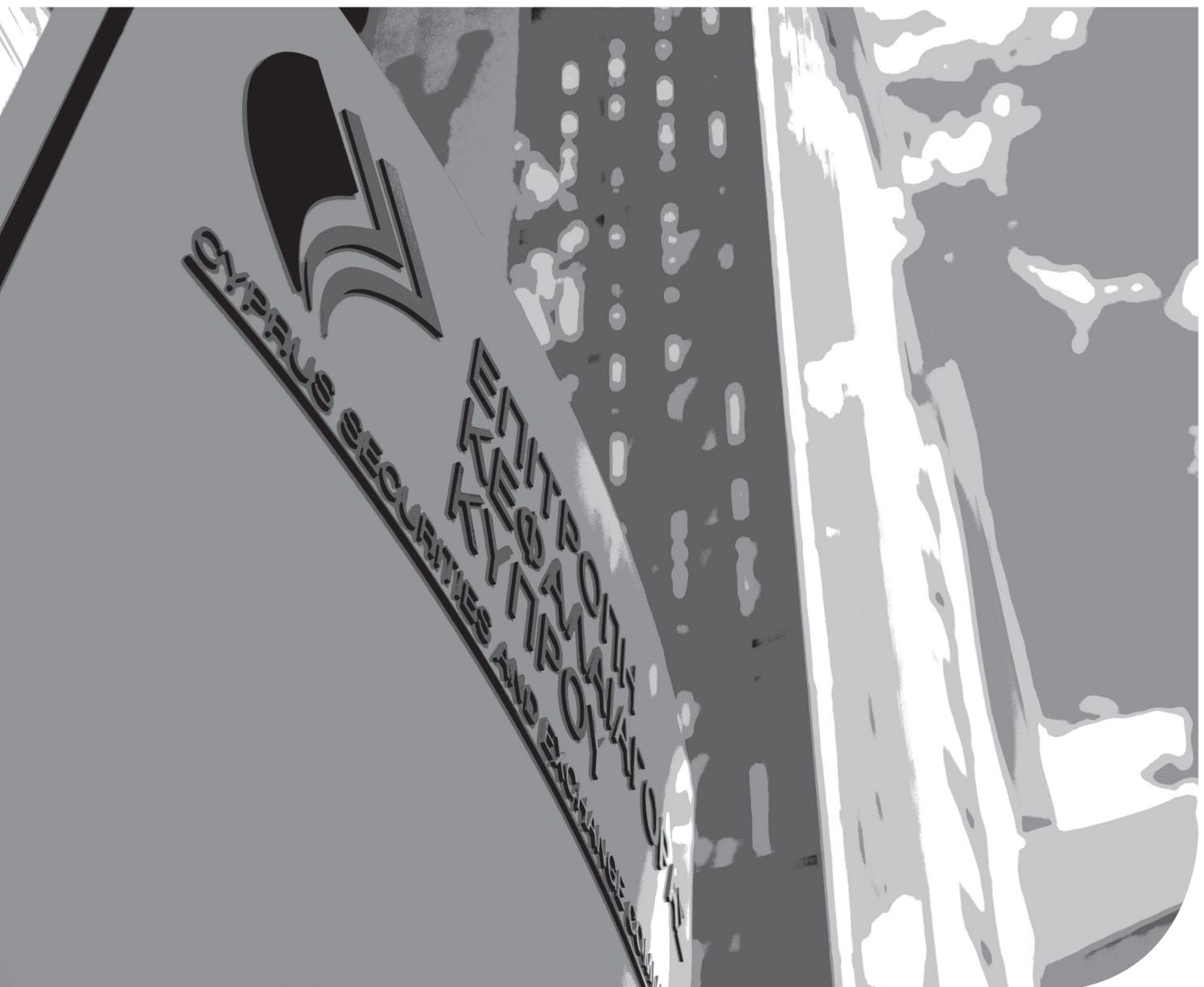
- Exercise better risk based judgment prioritizing regulatory activities
- Achieve efficiencies and better allocate

resources where risks are considered to be greater

- Strengthen its ability to take effective regulatory action where necessary
- Improve oversight and reporting on high risk regulated entities
- Develop evidence based policies using the knowledge obtained
- Take prompt and consistent regulatory action where necessary.
- However, the risk based approach, also benefits the regulated entities, which

now will:

- Have a better understanding and anticipation of the supervisory approach and its intensity that will be based on their profile, size and complexity of operations.
- Have frequent and open communication with the Regulator. Especially for higher risk entities, a Relationship Officer will be introduced who will be the point of contact on all supervisory areas concerned.
- Be benchmarked to other entities of similar size and characteristics.



AN OVERVIEW OF THE FRAMEWORK

The Risk Based Supervision Framework (RBS-F) is designed to ensure that risks are managed at a relevant level. This involves ensuring appropriate review, challenge and oversight of the risks bared by the regulated entities.

Below we provide the architecture of the risk model, its components, and how different parameters are combined to assess individual risks for each entity.

What risk refers to?

A risk for CySEC, is something which can cause harm to its statutory objectives. Each entity bares different risk which may relate to its:

- *External environment*, depending on the business model, the services and the market in which it operates.
- *Internal Environment*, depending on the governance arrangement, policies, procedures and systems implemented.

All the above, are closely linked to the regulated framework relevant to each entity and its arrangements to achieve compliance with its regulatory obligations, aiming to minimize such risks.

Identifying and assessing risks, is a process that CySEC will perform on an on-going basis, and for which will use and derive information from:

- Regulatory returns
- On-site reviews
- Market practices and economy performance
- Investors / customers

- Other regulators (especially within the EU).

Initially, each entity's **inherent risk** will be calculated based on *quantitative information* provided from regulated entities. This however will be gradually enriched with more *qualitative information* on each entity's processes and adequacy of controls. Therefore, entities will have the opportunity to decrease their risk level, once they prove to CySEC that they have adequate controls to mitigate their inherent risks.

CySEC's Risk Appetite

We define our supervisory approach based on our risk appetite and the supervisory framework is designed to allow closer monitoring of those cases which may generate a risk that is outside our appetite.

The methodology was established to allow and identify those regulated entities which warrant more intensive supervision. It is acceptable that risk cannot be entirely eliminated, while some of the risks accepted or that are not eliminated, may lead to failures.

The size of each entity gives a significant indication of risk, since the impact of failure of bigger entities is expected to be higher. Therefore, entities which are categorised to be of higher risk for CySEC, do not necessarily mean that their controls are inadequate or that they have significant malfunctions, but may also indicate the importance of these entities within the market due to their size. Therefore, bigger entities are expected to be more closely monitored than smaller ones.

However, regardless of an entity's size,

in cases where there are indications that the probability for an entity’s failure is significant, CySEC will also exercise enhanced supervision and closer monitoring.

The components of the RBS-F were designed to capture and assess these two indicators (i.e. **impact and probability**) in a manner that is comparable amongst all regulated entities.

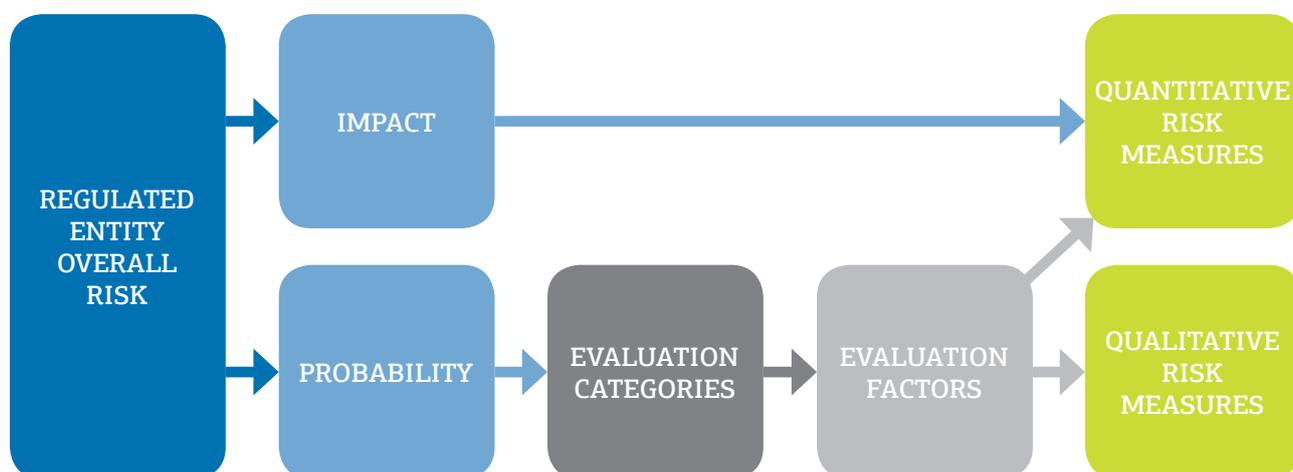
How does the model work?

Each entity’s overall score is calculated along specified assessment criteria and with the use of an IT support system that provides a standardised framework. The analysis combines the tools of offsite and onsite reviews.

We consider and assess risk for each regulated entity as a combination of:

- **Impact** (i.e. the potential harm that could be caused) and
- **Probability** of failure (i.e. the likelihood of an event / issue occurring).

Diagram 1



As illustrated in the diagram above, the assessment of an entity is based on a comprehensive and pre-defined set of “quantitative” and “qualitative” criteria / risk indicators, referred to as “risk measures”, which allow the risk assessment to be performed in a consistent manner and facilitate comparability amongst regulated entities (of the same type).

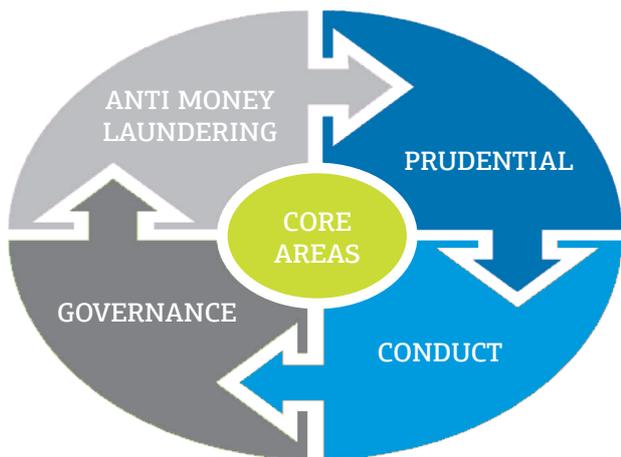
- **Impact** is measured in a way that mainly captures *the size of an entity* and thus measured using quantitative risk measures. Impact is calculated using numerical data extracted mostly from regulatory returns.
- **Probability** assesses *the likelihood for a certain risk / event to occur* for a regulated entity. The risk measures developed for the assessment of probability are grouped into a list of “Evaluation Factors”, which are in turn grouped into “Evaluation Categories”. Probability derives as the relationship amongst different components, as these are defined and illustrated in *Diagram 3*.

For the purposes of the risk assessment, CySEC will focus on each of these components, by obtaining and analyzing both quantitative data and qualitative information (i.e.

understand the entity's way of operation, controls and other arrangements).

Probability can be assessed under four (4) different *evaluation categories*, aim of which is to capture a different group of risks:

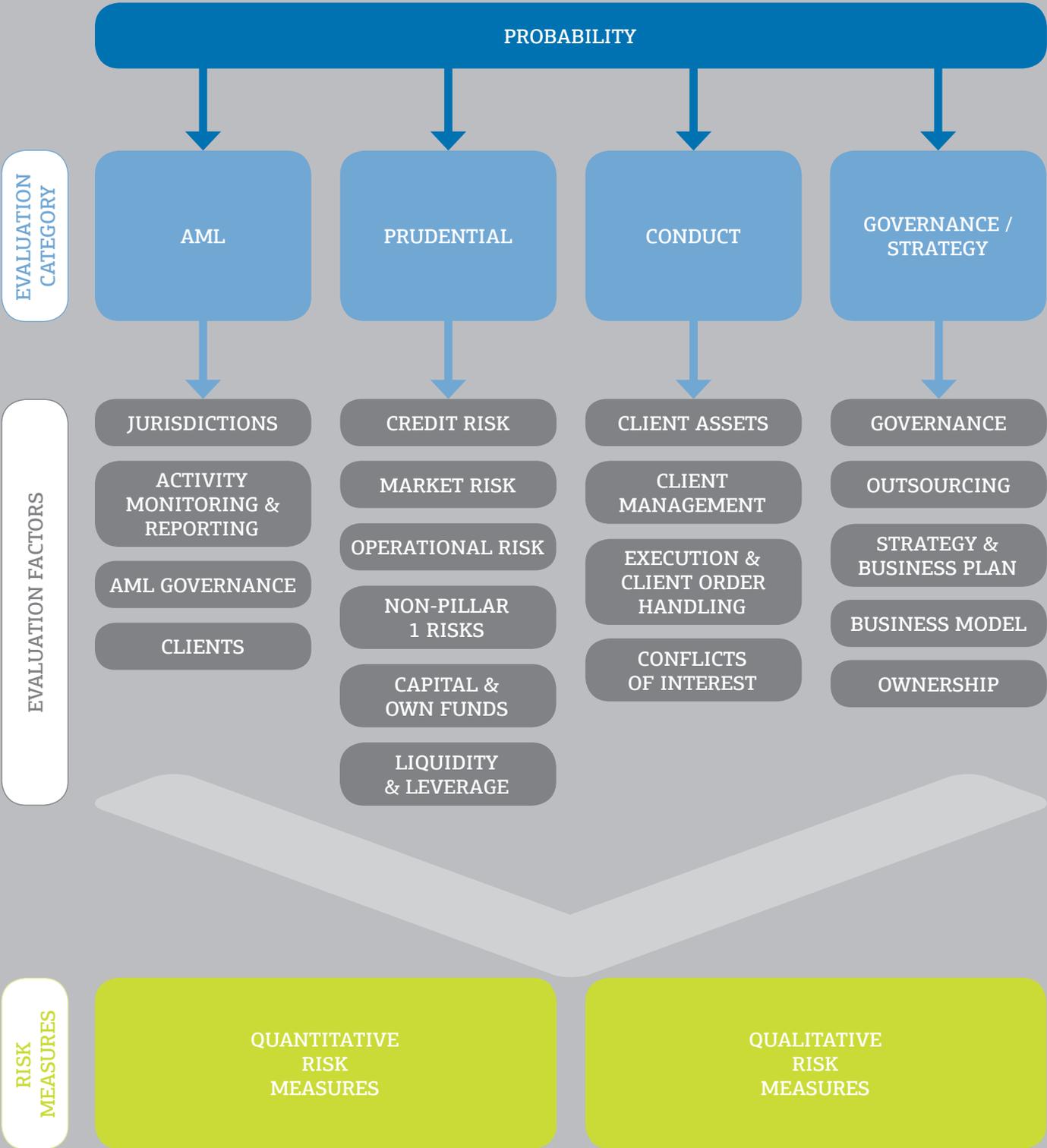
Diagram 2



1. **Anti-Money Laundering:** Aim is to ensure that regulated entities minimise the possibility that they may be used for financial crime.
2. **Prudential:** Aims is to assess the safety and soundness of the regulated entities and reduce the threat entities pose to the stability of the financial system in providing critical financial services.
3. **Governance & Strategy:** Aims is to assess whether processes and decisions that seek to define actions, grant power and verify performance of the entity are adequate.
4. **Conduct:** Aim is to ensure that clients get a fair treatment and ensure that markets are resilient and fair.



Diagram 3:



It is noted that depending on the type of entity, i.e. whether it relates to a Cyprus Investment Firm (CIF), an Administrative Service Provider (ASP) or a Management Company (MgtCo), the assessment components may differ, as applicable. The applicable evaluation categories, per type of entity, are as follows:

- **CIFs:** Entail risks arising from all four areas covered by the evaluation categories described above, and hence are assessed accordingly.
- **Management Companies:** Probability of failure is evaluated on AML, Governance and Conduct risks.
- **ASPs:** Only the AML risk is evaluated, as this is considered the key area of concern for CySEC in this industry.

Applicable Evaluation Categories
CIFs
Governance and Strategy
AML
Prudential
Conduct

ASPs
AML

Management Companies
Governance and Strategy
AML
Conduct

Each evaluation category is assessed based on a pre-defined set of **evaluation factors**, which capture similar risks, as indicated in *Diagram 3*.

Evaluation factors are assessed based on risk measures which fall under a common area of the regulatory framework that governs the supervised entities and thus,

capture similar risks. A structural method to combine the ratings of each entity's risk measures is used to rate each evaluation factor.

Probability is assessed both quantitatively and qualitatively, depending on the stage of the risk assessment and the risk rating of the entity.

Quantitative Probability aims to capture the inherent risk of failure within an entity through quantifiable risk measures, using data derived from the regulatory returns of the regulated entities.

Qualitative Probability is mainly captured through the assessment of controls within the regulated entities, as well as the review of the processes and procedures in place.

Entity Overall Score

An entity's overall score indicates the importance of each entity to CySEC and is calculated as a combination of its impact and probability.

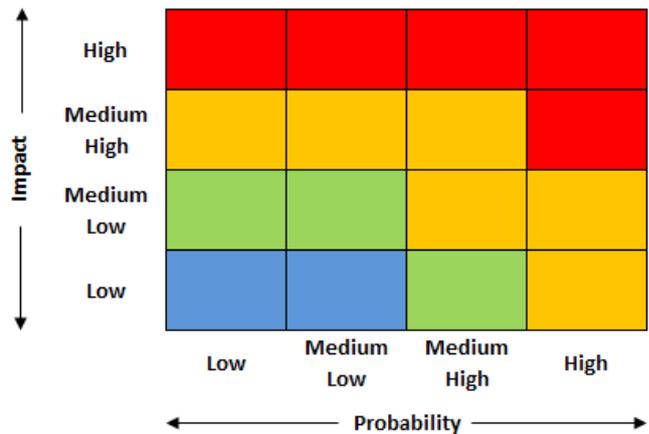
We will score each entity in four (4) categories (the supervisory stances): Low (L), Medium-Low (ML), Medium-High (MH), High (H).

ENTITY SUPERVISORY STANCES (overall score)	
	High
	Medium High
	Medium Low
	Low

Based on risk appetite, we have defined how the combination between the two would result to each entity’s overall score. As already explained, we consider that bigger entities are more significant, and therefore, regardless of their probability rating, will be categorised as “High” and thus will be closely monitored. It does not necessarily mean that a high rated entity is also a high risk entity, however, it does mean that CySEC cannot afford this entity to fail, and therefore will pursue closer monitoring.

Diagram 4 below illustrates the relationship of impact and probability to define an entity’s overall score:

Diagram 4:



For example, an entity that is of high impact, will be scored as high, irrespective of its probability of failure. Entities whose probability is rated as high, may be scored either as High or Medium High, depending on the entity’s impact.



ENTITY STANCES AND APPROACH TO SUPERVISION

In line with the RBS-F, the approach and intensity of supervision is proportionate to the importance (and thus overall score) that each entity poses to our objectives.

The profile of each entity will define the supervisory approach that will be followed, meaning the intensity of supervision and the areas of focus.

Simpler methods of supervision can be applied in the case of institutions that do not pose major risk to CySEC's supervisory goals. Such differentiation may apply to supervisory methods, the depth and scope of supervision.

Based on the entity overall score the intensity

of supervision varies as per the table below:

With the RBS-F, the concept of Relationship Managed firms is being introduced for H and MH firms. A CySEC Officer is allocated to each firm (i.e. the **Relationship Officer**), who will act as the point of contact between CySEC and the regulated entity.

H and MH should expect to have more frequent communication with CySEC, while aim is that the Relationship Officer will have a good understanding of the entity's business model and the key risks arising. These entities will be prioritised in CySEC's supervisory/monitoring programme so that to comfort that no significant failures will arise.

Supervisory Stance / Entity Overall Score	Approach	Description / Approach to supervision
H	Relationship managed	Establishment of a supervisory programme that is designed to enable each of the Probability Ratings to be assessed through regular meetings, targeted reviews and tailored remediation plans.
MH	Relationship managed	A regulatory approach consistent with the one followed for H risk entities will be applied. However, in order to ensure appropriate application of the RBS-F principles, the supervisory programme for MH risk entities will be <i>less frequent / rigorous</i> than the one for H risk entities.
ML	Thematic reviews	Subject to desk-top data analysis and potential selection for thematic review. ML risk entities will be prioritized for thematic reviews where probability scores show they are relevant to individual entities.
L	De minimis	Limited interaction beyond administrative supervisory processes/ supervision through reporting. Random selections for desk-top data analysis that could potentially result to thematic reviews.

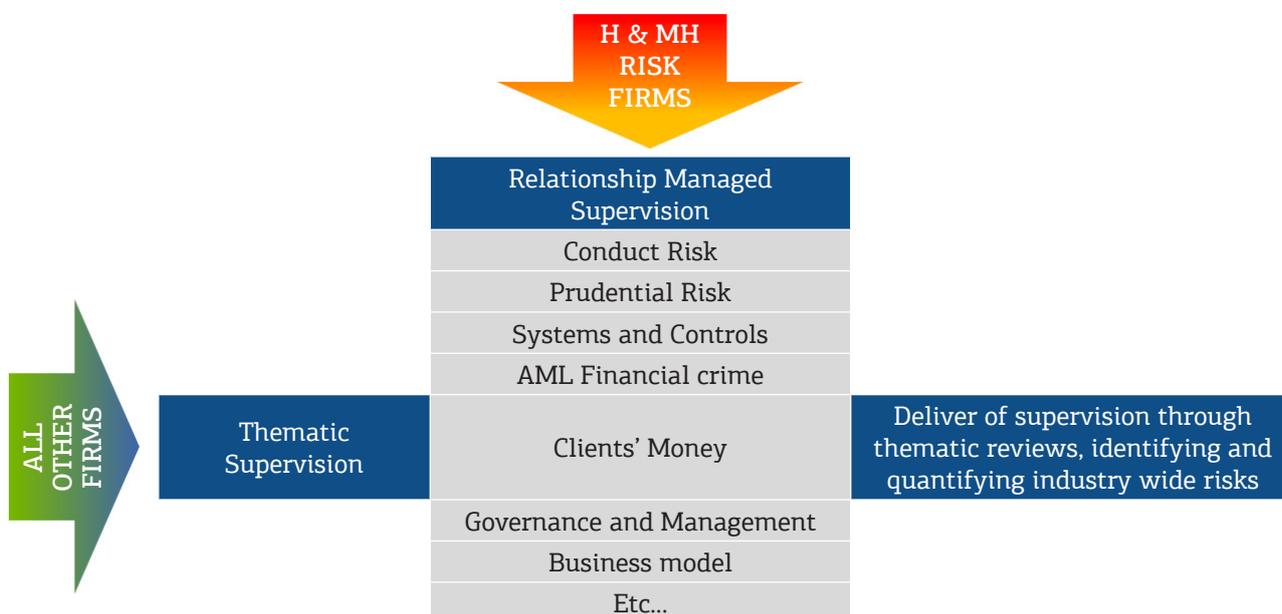
It is noted that CySEC adopts a two-dimensional approach to monitoring:

- **Vertical Supervision:** Assess and review the risks on an entity level, i.e. “firm specific supervision”.
- **Horizontal Supervision:** Look at certain thematic areas across the market that impose a common risk and identify trends on specific areas, i.e. “thematic reviews”.

The thematic areas may derive and scope at a small peer group of firms potentially facing similar issues, or cover a larger scale of entities across the market.

For thematic work, often a sample of entities will be selected, either based on the areas they pose to have their most significant risks, or which is representative of the different sizes or structures in the market. This may include some firms which we think are likely to implement the highest standards in terms

Diagram 5:



While H and MH firms are subject to both, horizontal and vertical supervision, ML and L firms are mostly subject to horizontal supervision (i.e. thematic reviews), either on-site or off-site.

During our supervisory work, your firm may be subject to **thematic reviews** that we undertake on specific issues. For ML and L entities, which have no dedicated Relationship Officer, almost all of our reviews will be carried out on a thematic basis. Thematic reviews also play a significant role in the supervision of H and MH firms.

of systems, controls and practices, so that we are in a position to benchmark to good practices across the market.

It is noted that all entities will be subject to the basic monitoring procedures which involves analysing their regulatory returns submitted to CySEC. For low risk firms, the majority of supervisory responsibilities will be performed off-site, via the review of such returns, which will be provided to CYSEC either on a regular or ad-ho basis.

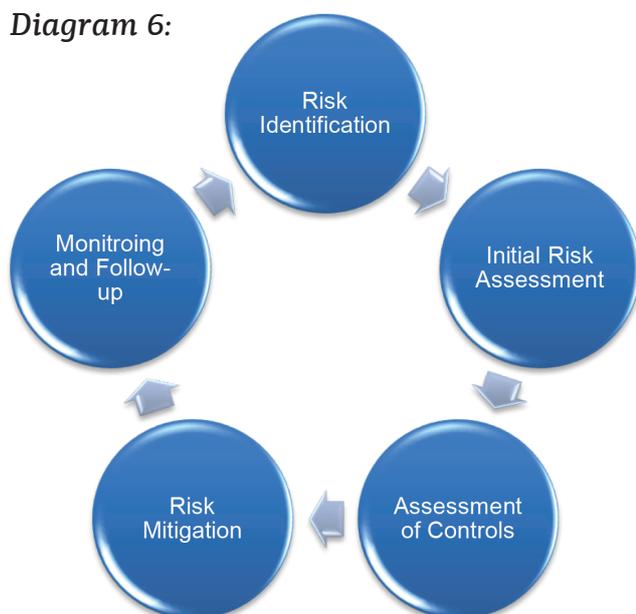
HOW RISK BASED SUPERVISION WORKS IN PRACTICE

The RBS-F is the link between our statutory objectives and our regulatory / supervisory activities, and is designed to:

- Identify the main risks to our objectives.
- Measure the importance of those risks.
- Mitigate significant risks identified.
- Monitor and follow-up the progress on mitigation actions, where defined.

We regularly review the amount of risk we are prepared to accept (i.e. risk appetite) and focus our resources on the risks that matter most. The results of the assessment will evolve throughout the supervisory cycle which is designed to be continued for each entity (i.e. this is not a one off exercise that occurs on a certain point of time during the year, but will be informed on an ongoing basis from the supervisory results and events which might occur). Our supervisory cycle is as follows:

Diagram 6:



Risk Identification

During this phase, we aim to identify the key risks deriving from the market and ensure that our framework is tailor made to capture and assess those risks.

At this stage, all regulated entities are required to submit a set of information/data that will facilitate such analysis. Of course, our risk identification process includes other sources of information, such as the regulatory framework, best practices in the financial services sector, trends followed in the European environment as well as the general macro and micro economic environment.

Initial Risk Assessment

This process is performed internally within CySEC on an **annual basis**, and includes the assessment of each regulated entity's inherent risk.

This is performed based on information/data already available to CySEC, deriving from your regulatory returns (submitted recently or during the previous years) as well historic trends of your entity.

Following a comprehensive analysis of data / information available and the processing of such data/information to identify unusual conditions, we will define each entity's inherent risk, and also obtain a general picture of the market.

This stage is mostly for planning and is designed to give CySEC an initial estimate of the level of risk. Therefore, based on the results from the initial risk assessment, we will define our supervisory approach and program for each entity.

Assessment of Controls

This is the phase where CySEC's supervisory approach is to be implemented in order to validate the results of the initial risk assessment performed during the previous phase.

Regulated entities, at this phase have the opportunity to present to CySEC their approach and business model and how controls are implemented to mitigate the risks that occur.

Interaction with regulated entities will be established to perform both on-site and off-site reviews, the frequency and depth of which will vary, depending on the area of review and the profile/supervisory approach defined for each entity.

Different approaches will be followed from CySEC for gaining a better understating of the entity, its risks and controls established, amongst which include:

- **On-site reviews:** on-site visits to your firm may take place to fill-in gaps in our knowledge and investigate any specific areas which may pose risks to our statutory objectives. The Relationship Officers appointed for your firm will normally carry out the visits, possibly with the support of subject matter experts, where this is deemed necessary.

It is noted that the purpose of the on-site visits, is to identify where your business or controls structure may give rise to material risks to our statutory objectives, therefore, on-site visits may not take place if we feel we already have enough information on these areas.

- **Meetings/Interviews:** Meetings and interviews with key persons within your firms may need to be planned and take place, either during an on-site review, or

ad-hoc in case we need to discuss certain matters with you and obtain specific information.

Meetings will usually be held with the entity's Senior Management or people who hold key positions, such as the Head of Departments and persons responsible for the control functions of the entity.

- **Queries:** Specific queries may be communicated in writing, for your firm to provide relevant information and/or clarifications as applicable. Usually, a timeline will be set for your firms to prepare and submit a response to our queries. Additional clarifications may also be requested, if deemed necessary.
- **Regulatory returns review:** Information submitted as part of your regulatory returns, as these derive from your reporting obligations in line with the regulatory requirements, are reviewed and assessed by CySEC. Such information, include amongst other, the annual reports from the key control functions and AML, the monthly prevention statements, the financial statements, ICAAP, CoREP, suitability report on clients' assets etc. Following the review, we may communicate with you in order to further understand and assess specific issues that may arise.

Aim is that the results from our supervisory program will be communicated to you in a manner that you will have the opportunity to explain key issues raised and correct any errors of facts raised.

We aim that the intensity of risk management program and supervisory approach is proportionate to the risk profile that your firm poses to CySEC, both in terms of impact and probability.

The results of this phase will be taken into consideration for proceeding with the assessment of controls and are used as input in our initial assessment of your entity's probability in order to ensure that a more complete picture of your entity's specifics and risks is captured and assessed. In this way, the controls and risk mitigation actions implemented by your firm will be taken into consideration for your overall risk assessment.

Risk Mitigation

From the output and conclusions of our ongoing monitoring and supervisory program, it is possible that we propose to your firm a risk mitigation program, with certain actions that need to be taken in order to minimize the risks we consider you are exposed to and may bear a significant effect on our statutory objectives.

The risk mitigation and remediation program defined from CySEC for your firm

to implement, in order to mitigate its risks identified, is the result of both the initial risk assessment and the assessment of controls.

Depending on the significance and criticality of the issues raised, the mitigation program may vary.

Monitoring and Follow-up

Regulated entities should expect that CySEC will monitor the implementation of corrective actions (i.e. the risk mitigation and remediation program set). The response from you on this matters is of great importance and will be taken into consideration during the assessment of controls and the overall risk assessment of your firm.

If we believe that issues are not adequately or promptly addressed from your firm, we may consider whether the firm has breached any regulatory requirement and consider whether any other formal actions will need to be taken (such as enforcement actions).

