association of the luxembourg fund industry

guidelines

Operational Risk Management within UCITS

in association with ALRiM LUXEMBOURG

table of contents

I. introduction

EU regulation, as implemented in Luxembourg as the Law of 2010 and CSSF Regulation 10-4, has focused attention on the requirement for management companies pursuing the activity of management of a UCITS and investment companies that have not designated a Management Company (Self Managed SICAV) to have in place an adequate Risk Management (RM) function that is proportionate to the business conducted by those companies and the risk profiles of the UCITS which they manage.

The ALFI document "Best Practice Proposals for the Organisation of the Risk Function of a UCITS Management Company or UCITS Investment Company" suggested a set of best practices that the Fund Directors and Senior Management of Management Companies and Investment Companies may wish to consider when developing or reviewing the adequacy of their RM functions.

Such RM function is required to establish, implement, and maintain an adequate and documented risk management policy which identifies all the material risks that the UCITS management companies or investment companies are or could be exposed to, including, inter alia, all operational risks that may be relevant for each UCITS they manage.

The aim of this document is to present best practice proposals for the management of Operational Risk and to assist Board members and senior management in the development of their RM functions by:

- Highlighting the key sources of legal and regulatory guidance in relation to RM in order to get a common understanding thereof;
- Proposing a set of best practices regarding:
    - The identification of all relevant operational risks to which the UCITS are or may be exposed;
    - The measurement and management of these identified operational risks; and;
    - The reporting with regard to these risks and related information to senior management and the Board by the RM function.

Throughout this document the term "ManCo" will be used to refer to a management company or a self managed investment company where no management company has been designated.

II. key legal and regulatory framework

In relation to risk management a number of laws and regulations have been issued on European and Luxembourg level.

The table below, details a brief overview of this framework including a non-exhaustive list of the key laws and regulations related to risk management.

Legislation and Regulatory Framework for Risk Management		
	European Union	Luxembourg
Level 1 legislation	Directive 2009/65/EC	Law of 17 December 2010 on Undertakings for Collective Investment (2010 law replaces the 2002 law)
Level 2 implementing measures	Commission Directive 2010/43/EU	CSSF Regulation No.10-4
Level 3 guidelines	ESMA Guidelines 09/178 ESMA Guidelines 10/788 ESMA Guidelines 11/112	CSSF Circular 11/498 CSSF Circular 11/512 CSSF Circular 12/546

The additional guidelines listed below are also relevant best practice documents, which may be considered for the implementation of an operational risk framework:

- Best Practice Proposals for the Organisation of the Risk Function of a UCITS Management Company or UCITS Investment Company; and;
- Guidance Paper for the Risk Monitoring of Functions Outsourced/ Delegated by a Management Company or Investment Company.

These guidelines, produced by the ALFI Technical Committee, seek to provide a set of best practices that the Boards and Senior Management of Management Companies and Investment Companies may wish to consider when developing, or reviewing the adequacy of, their RM functions and considering the risk monitoring of delegated functions.

Industry Guidelines	
Best practice guidelines in other industries	• **Sound practices for the Management and Supervision of Operational Risks** issued by the Basel committee on Banking Supervision, February 2003; • **The Compendium of Supplementary Guidelines on implementation issues of operational risk** issued by CEBS/EBA September 2009.

III. risk management and operational risk

This document focuses specifically on the identification, monitoring and reporting of Operational Risk.

Operational Risk is defined in CSSF Regulation 10-4 as the "risk of loss […] resulting from inadequate internal processes and failures in relation to people and systems of the management company or from external events, and includes legal and documentation risk and risk resulting from the trading, settlement and valuation procedures operated on behalf of the UCITS". Management of Operational Risks aims to reduce or eliminate the impact of these types of risk on the successful operation of the business.

The requirement for a formal coverage of Operational Risks for ManCos and Investment Companies are derived from the UCITS IV directives 2009/65/EC and 2010/43/EU and the Luxembourg CSSF Regulation N° 10-04. According to Luxembourg regulation, the Risk Management Process (RMP) should comprise procedures necessary to assess "… the exposure of the UCITS to all other risks, including operational risks, which may be material for each UCITS it [the ManCo] manages."

CSSF Circular 12/546 (clause 7.1.4) requires that "every use of an external service provider must be preceded by written due diligence by the management company on the provider.

In the context of this requirement of diligence, the management company must, amongst others, identify the operational risks deriving from this delegation".

ManCo and Fund Boards are responsible for defining the risk appetite of the business and approving the risk profile of the funds that they manage. Additional guidance may be found in the ALFI guidance document on CSSF Regulation 10-04 entitled "Best Practice Proposals for Management Companies or UCITS Investment Companies". Senior management must ensure that the operational risk framework is implemented fully and efficiently.

The RM function is responsible for the design, implementation and ongoing development of the operational risk framework and has to ensure that adequate policies and procedures do exist. All parts of the business are exposed to forms of operational risk and a risk management framework therefore needs to be embedded across the business to be fully effective. In fact, operational risks are primarily managed at business levels by having implemented defined processes and related internal controls ("1st line of defence"). It is worth noting that in large organisations individual business departments may have dedicated risk functions themselves, which not only support their part of the business but provide useful information and support to the overall RM function.

Layers of the internal control system

The RM function as an independent function provides, together with the Compliance function, for a 2nd line of defence (which is accompanied by Internal Audit as the 3rd line of defence).

The responsibility of the RM function concerning operational risks is to provide an independent assessment of the operational processes and related internal control framework in place to identify potential risks for the funds and the company. Business management in conjunction with RM will ensure that operational risks are adequately measured, monitored and managed. In its independent role, risk management will actively engage in discussions with the business to better understand processes and control procedures implemented (to be able to challenge and highlight potential weaknesses). They will ensure the timely and appropriate escalation of risk issues to senior management and the Board. RM may use and aggregate data and information collected by the business, for example, RM may receive KPI information that are produced/collected by the various business functions that may help RM to identify potential risks that require remedial measures. This monitoring, together with Compliance, is the second level of defence. Later in the document we will consider how RM may independently identify, monitor and escalate risk issues.

In relation to the responsibilities of the ManCo the internal control, independent risk management and oversight by the supervisory body of the UCITS is shown diagrammatically below.

Operational risks arise in the three functions for which the ManCo is responsible:

- Investment Management;
- Administration; and;
- Marketing (Distribution).

Such risks will be mitigated by internal control processes within the operational policies and procedures which the ManCo has in place and which they apply to the daily operations of the ManCo.

Delegates should have equivalent policies and procedures that are in line with the internal control standards set by the ManCo. These are the first level line of defence. Later in this document we will look at examples of the operational risks that are relevant to ManCos and the UCITS that they manage and we will consider the mitigating controls that may be put in place.

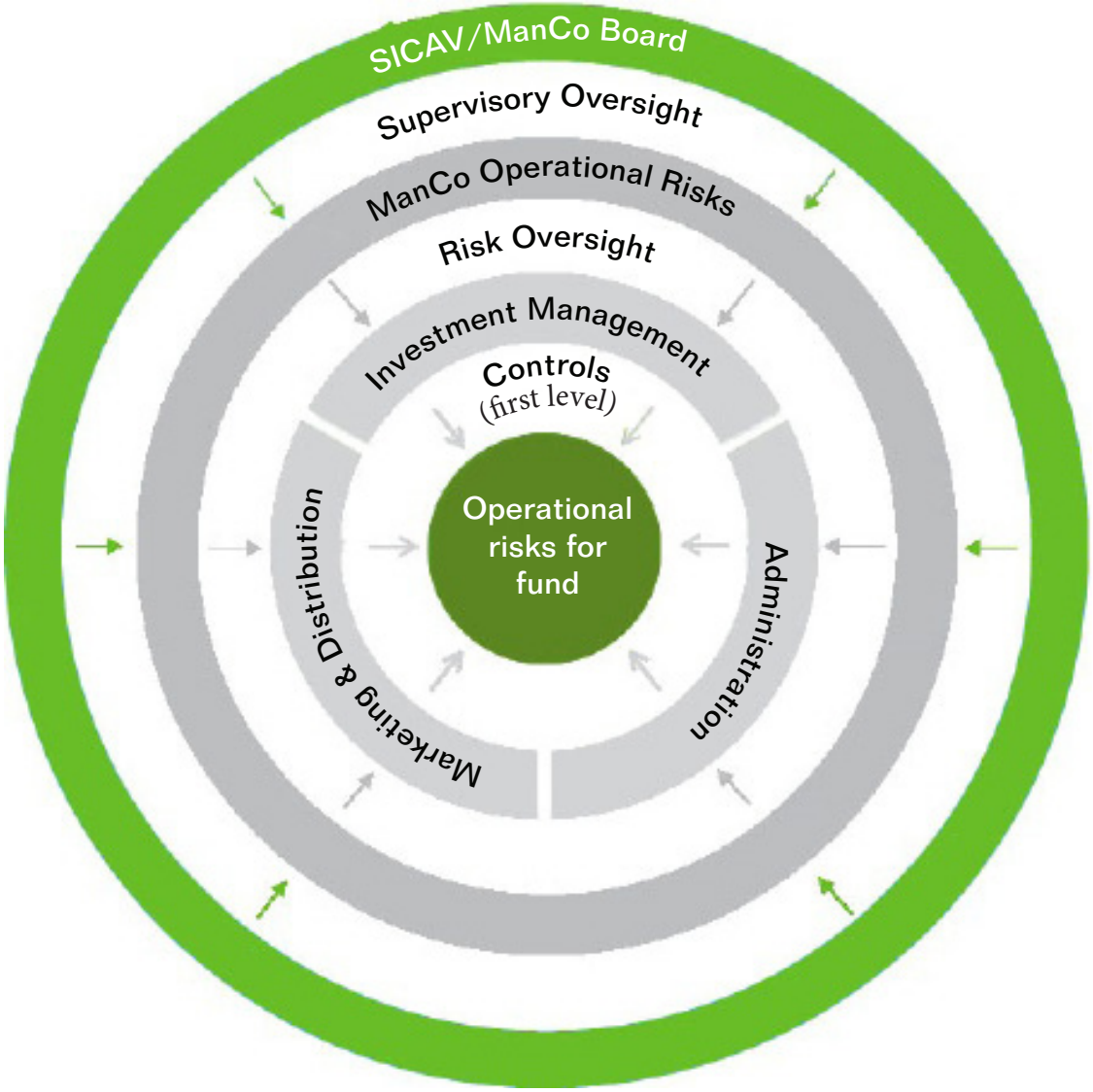
Senior Management of the ManCo will typically be involved in the RM process either in a supervisory or oversight role, by assuring that the required regulatory tasks are performed in an appropriate manner and by monitoring the proper implementation of the documented RMP. They will also be the first point of escalation for all RM matters and provide regular reporting to the Board of Directors.

The ManCo Board of Directors will supervise that the RM function is operating effectively and remains appropriate and proportionate to the business of the ManCo and the UCITS managed.

Specifically the Board remains responsible for:

- Definition/approval of the company's risk principles;
- Authorisation of Senior Management to set up the RM function;
- Promote the development of risk measures;
- Periodic review of effectiveness of the RM function;
- Review of how the company manages risk;
- Act as a direct line of escalation;
- Approve the documented RMP.

Collectively the Board, Senior Management and the persons appointed to conduct risk management must have the competencies to understand and to be able to identify, measure and manage the operational risks in the ManCo and the UCITS that they manage.



1. Categories of Operational Risk

Operational risks are generally classified in four categories, see chart below, split between internal (process, people, systems) and external events.

Below we will look at generic operational risks, under these four categories, and then consider examples of those operational risks that are relevant to ManCos and the UCITS that they manage.

Cause	Potential Risk Event (What could go wrong) - Examples	Potential impact
Internal events • Process • People • Systems	• **Organisational/Process** e.g. Inadequate procedures • **People** e.g., Failure to follow procedures • **System/IT Infrastructure** e.g., Unauthorised access	Financial loss Customer claims Near misses Forgone revenue Regulatory fines Reputational damage
External Events	Outsourcing Risks Fraud Market Events	

2. Examples of generic operational risks

Below are examples of generic operational risks and their mitigants. This is not an exhaustive list, but should be used as a guide to the types of risks and risk categories a Risk Manager should assess for their organisation.

Potential Risks	Risk Mitigants
Organisational/Process Risks These risks are due to non-optimal organisational structures; inadequately designed processes or internal control systems; or the lack of sound project management.	
• Inadequate or incomplete procedures; • Inadequate or inappropriate change management; • Lack of internal control reviews; • Undocumented or unreported breaches; • Lack of segregation of duties.	• Policies and procedures are documented and subject to regular review by management; • Changes to operating models and IT systems are controlled by detailed project governance; • Management regularly review the effectiveness of Risk Management and Compliance and ensure regular internal or external audits are conducted; • Clearly defined organisational hierarchy in place with procedures for regular reporting and error escalation.
People Risks Examples of people risk are unintentional errors; a lack of adequate or sufficiently trained staff; fraud/criminal activities by employees	
• Lack of capacity planning; • Key person dependencies; • Weak or ineffectual management; • Undetected money laundering or theft; • Un-escalated errors; • Insufficiently skilled staff; • Fraud.	• Management regularly review the adequacy of staff levels and their skills set; • Succession planning for key roles is in place with training to meet development needs; • Access to all systems has to be approved and regular recertification is in place; • Segregation of duties in place to ensure no one person is responsible for a transaction; • Systems designed to enforced dual control through re-keying, or similar controls; • Established Code of Ethics/Business conduct rules; • Established escalation protocols; • Risk awareness training for all staff.

Technology/IT related/Infrastructure risks Technology risks can be due to defective, unavailable, or inadequately secured technical resources/IT systems	
• Inadequate access controls; • Lack of business continuity planning and testing; • Inadequate systems; • Lack of system maintenance and monitoring; • Vendor failure; • Lack of system security.	• Strict application of password controls and regular re-certification of users; • Documented BCP in place with regular testing performed; • Defined and documented IT policies; • Regular system maintenance and monitoring; • Vendor management; • IT protection against external threats (unauthorised access to company network).
External factor risks External factors can be inappropriate external services/outsourcing, external criminal activity or disasters affecting the business	
• External fraudulent activities; • Natural disaster; • Geo-political risks; • Market events; • Vendor risks.	• Resiliency management; • Crisis management exercises; • Internal security; • Insurance coverage; • Vendor contracts, due diligence and on-going monitoring.

IV. operational risks specific for UCITS funds

From the perspective of a ManCo, the UCITS they manage and the investors in the UCITS, Operational Risks may arise as part of the provision of the Investment Management, Administration and Marketing functions which are the responsibility of the ManCo to provide.

Below are some examples of the types of risks that senior management of the ManCo may wish to consider when developing their RM function and the RMP. While these operational risks are relevant to ManCos and UCITS each ManCo will need to assess the likelihood of these risks arising based on the operating model of their company and, where appropriate, that of their delegates.

For example, if the ManCo operates a fully automated Investment Guideline Restriction system that prevents trading instructions being placed that do not conform to the investment mandate of the UCITS there will be significantly less possibility of an investment breach occurring than if the control is only performed manually. Therefore the controls and monitoring around this risk would need to be modified accordingly.

Examples of Operational Risks applicable to UCITS Funds

Investment Management	Examples of Mitigating Controls
• Investment activity not managed in accordance with the Fund's documentation and applicable regulation; • Delegation to the Investment Manager is not covered by a legal agreement; • Guideline monitoring procedures are not adequate; • Investment transactions are not properly executed or settled; • Corporate actions are not correctly handled; • Investments are not properly registered and/or client money is not segregated; • Investment transactions are not correctly, or timely, recorded in the Fund Accounting records.	• Reviews conducted of investment activity independent of the Investment Manager; • Investment Management Agreement signed between the ManCo and each delegated IM; • Investment Guideline Monitoring in place that is independent of the IM function with escalation to the ManCo; • Controls verifying eligibility of assets; • Reasonable level of straight through processing and automated validation controls; • Reporting of unsettled securities transaction, reconciliation of broker confirmations; • Implementation and management review of exception reports; • Segregation measures for client assets.
Administration – Fund Accounting	
• UCITS assets are not valued independently and accurately with current market prices; • NAV of the UCITS are not accurately calculated and/or reported in a timely manner; • Inaccurate calculation and/or accrual of fund fees and expenses; • Failure to reconcile Fund Accounting records to the Custodian records; • Investment income and tax calculations are not accurately recorded, or recorded in a timely manner;	• Independent valuation controls; • Review of NAV evolution compared to a relevant benchmark; • Management/Valuation committee review of significant valuation estimates; • Review of fund expenses compared to expectations, and follow up of deviations; • Reconciliations between fund records and custodian records, and timely follow up; • Reconciliations between tax calculations and books and records; • Management review of exception reports, financial statements.

• Annual/Semi-Annual reports and accounts are not prepared in accordance with disclosure requirements and/or not submitted within regulatory deadlines.	
Administration – Transfer Agency	
• Accounts opened without proper client identification and completion of documentation; • Trading cut-off times not respected, permitting market timing/late trading; • Client transactions are not processed in a timely and/or accurate manner; • Failure to maintain the UCITS register in an accurate and timely manner and to perform regular reconcilements; • Changes to client data are not properly authorised or updated in a timely manner; • Cashflow forecasts not provided to the investment manager in a timely and/or accurate manner.	• KYC/AML documentation – verification of completeness and relevance of documentation; • Keeping documentation up to date with changes in regulations and best practices; • Trading cut off verification controls; • Review of exception reports over capital transactions processing; • Controls for maintaining client data up to date; • Review of exception reports, missed reporting deadlines etc.
Marketing (Distribution)	
• Delegation to distributors not covered by a signed legal agreement; • Distributors do not fulfil their responsibilities with regard to AML/KYC checking; • Suitability/Appropriateness obligations are not completed by distributors; • Failure to register/notify funds/share classes in a jurisdiction before starting to market the UCITS; • Failure to comply with host country marketing regulations/material requirements; • Non-compliance with appropriate inducement regulations in different jurisdictions.	• System for verifying completeness of distribution agreements; • Due diligence procedures over distributors, using a risk based approach; • Review of exception reports; • Review of blocked accounts; • Review of client complaints and proper follow up; • Establishing system for keeping abreast of key changes in local regulatory requirements, and ensuring proper follow up where necessary; • Establishing contact with local regulators/advisers where necessary to clarify understanding for significant areas which are unclear.

V. tools to assist with the assessment, monitoring and tracking of operational risks for UCITS

When looking into the operational risks that are relevant for each UCITS, the risk management function will need to define respective measurement and monitoring approaches for each risk category based on an analysis of the risks in the operational processes applicable to each fund. They will need to consider whether appropriate, and effective, mitigating controls have been identified and implemented in the ManCo, or its delegates, procedures in order to control the identified risks.

The RM functions should then consider what independent monitoring needs to be put in place to ensure that these controls are working and that timely escalation and reporting is taking place.

Below you will find examples of how a simplified documentary overview of risk measurement and monitoring approaches for a risk category for each of the Investment Management, Administration and Marketing functions may look. The methodology used for the identification of the risk type categories, the assessment of the risk frequency and the estimated severity, shall all be detailed and documented. It would be good practice to document all relevant operational risks in a similar manner.

Risk Category		Identified Risk Type	Approach to measurement of risks	Entity/ department performing measurement of risks	Tool/ system used to measure risks (if any)	Appraoch to limitations of risks	Entity/ department responsible for monitoring of risk limitations	Frequency of monitoring of risks	Approach to remedial actions (i.e. Escalation of breach limits)	Risk type estimated occurrence (frequency)	Risk type estimated severity
Operational risks	Investment Management	Investment Guideline Monitoring	Pre-trade check Post-trade check Check to UCITS accounting records	Operations department located in the IM office but independent of the IM function	Guidelines monitoring system linked to investment management system Guideline Monitoring system linked to Fund Accounting system	UCITS specific investment guidelines/ limits as per fund documentation Regulatory limits applicable to the UCITS Internal guidelines as appropriate	Operations department Independent oversight of all breaches of risk management	At point of making investment decision (intra-day) Daily (post trade)	Daily escalation to RM of all breaches daily escalation to compliance of all breaches Escalation to the Board of ManCo and SICAV at next Board meeting unless determined to be a significant issue Escalation to auditors, custodians, regulator as required by regulation	Rare	High

V. tools to assist with the assessment, monitoring and tracking of operational risks for UCITS

Risk Category		Identified Risk Type	Approach to measurement of risks	Entity/ department performing measurement of risks	Tool/ system used to measure risks (if any)	Appraoch to limitations of risks	Entity/ department responsible for monitoring of risk limitations	Frequency of monitoring of risks	Approach to remedial actions (i.e. Escalation of breach limits)	Risk type estimated occurrence (frequency)	Risk type estimated severity
Operational risks	Administration	Inaccurate NAV calculation of the UCITS	Pre-release check of NAV calculation	Checking function within the fund accounting process		Materiality limits established by Luxembourg regulation for NAV errors	Oversight Department with the ManCo	Daily before release of NAV	Daily escalation to RM and compliance of all breaches	Frequent	High
			Comparison to NAV change to benchmark change	Oversight by the ManCo of the NAV changes		Variance thresholds established above which further investigation of the NAV calculation to be conducted	Independent oversight of all breaches by risk management and compliance		Escalation to the board of ManCo and SICAV at next Board meeting unless determined to be a significant issue		
			Comparison of NAV change to expected fund performance	Oversight by portfolio managers of the NAV and the fund performance					Escalation to auditors, custodian, regulator as required by regulation		

Risk Category		Identified Risk Type	Approach to measurement of risks	Entity/ department performing measurement of risks	Tool/ system used to measure risks (if any)	Appraoch to limitations of risks	Entity/ department responsible for monitoring of risk limitations	Frequency of monitoring of risks	Approach to remedial actions (i.e. Escalation of breach limits)	Risk type estimated occurrence (frequency)	Risk type estimated severity
Operational risks	Marketing Distribution	Delegation to Distributor not covered by a legal agreement	Risk based due diligence conducted on distributor before on-boarding	Risk based due diligence completed by sales function with support from legal and compliance deparments as necessary		Specific authorised signatures only allowed to sign agreements	Client on-boarding department within the ManCo	At time of each client on-boarding	Escalation to senior management of any request to on-board a client without a legal agreement	Unlikely	Medium
			Standard agreement template used for all distributors	Legal department to review appropriateness of the agreement		Approval processes for allowing non-standard clauses, or deletion of clause, from agreements					
			Legal review and signing of the agreement by a duly authorised person	Operations to ensure agreement signed before opening an account on the ManCo systems		Regular refresh of due diligence process with the distributor depending on the level of risk assessment					

Overall, controls need to take into consideration both quantitative and qualitative information.
A culture of risk management within a firm, lead by the Board and Senior Management is essential for Operational Risk Management to be effective. This requires the RM function to consider the use of a number of "tools" to fulfil their responsibilities, these may include, but are not limited to, the following:

- Policies and procedures, procedures manual;
- Risk Control Self Assessment (RCSA);
- Key Risk Indicators (KRI) or Key Performance Indicators (KPI);
- New Business/Risk Approval Process;
- Due Diligence for Delegates;
- Risk Event Database;
- Other (for example: procedure repository, control plan with the list of all existing controls and their results, …).

1. Policies and procedures, procedures maual

All the processes of the ManCo should be detailed in a comprehensive set of documented policies and procedures. The policy shall detail the high level description, scope and limitations of the processes whereas the procedures should be orientated towards practical use of the process, including print-screens of the applications used and operational details (e.g., workflow, timing, data used).

The procedures manual should contain the links to all the procedures.
All these documents shall be kept up to date in order to prevent any misinterpretation by the ManCo staff and ultimately to prevent any operational risk.

2. Risk Control Self Assessments (RCSA)

The ManCo should regularly conduct a self assessment of the completeness and effectiveness of their control environment. These RCSA are a template of the identified risks that are present in the ManCo processes and the controls that have been implemented to help mitigate those risks.

By completing the RCSA the management of the ManCo assess whether the identified risks are still valid and have any additional risks been introduced as a result of new funds and/or operational processes. They also should assess whether the controls are still valid and are operating effectively. RM will be involved in the RCSA process by ensuring that the appropriate risks have been identified and that the testing of controls has been correctly completed.

RM would then ensure that action plans are put in place for the remediation of any identified control issues and follow up to ensure timely completion of the plans. The status of the RCSA process and resulting action plans would form part of the reporting to senior management and the Board.

The ManCo may decide to rate the control environment using predefined rating and severity scales, for example, 1 (highest rating) to 5 (lowest rating) and High, Medium, Low severity and agree a benchmark for remediation. Higher rating control issues would be expected to be remediated in a shorter time period than those rated lower.

3. Key Risk Indicators/Key Performance Indicators

A set of well-defined Key Risk Indicators (KRI)/ Key Performance Indicators (KPI) is one of the starting points for a proper identification, assessment, reporting and management of operational risks.

KRI/KPIs must:

- Be specific, measurable and timely;
- Cover operational processes that may generate significant operational risks for the ManCo/UCITS;
- Address delegated functions as well as those performed in the ManCo;
- Include bench marks or traffic light ratings (e.g., green/amber/red or low/medium/high) and thresholds for any type of operational error should show realistic risk situation of the ManCo/UCITS to which the KRI refers;
- Be regularly reviewed to ensure they remain relevant.

Example:

Transfer Agent Function:	• Number of revised trades (Subs/Reds) (monthly); • Gains/Losses generated by revised trades (monthly).
Fund Accounting:	• Number of days with NAV release after scheduled time.
Distribution:	• Incomplete dealer documentation (% of all Dealer accounts).
Investment Management:	• Number of active breaches (monthly); • Monetary impact of breaches (monthly); • Number of passive breaches (monthly).

Additional examples of KRI/KPIs are given in Appendix I.

4. New Business/Risk Approval Process

RM should be involved in assessing the operational, and other, risks that are introduced into the ManCo business as a result of; taking on new fund mandates, implementing new systems or changes to systems, out-sourcing or delegation of functions and any other change to the business or operating processes that result in a change to the risk profile of the ManCo business.

Before agreeing to the acceptance of the change or new business RM, together with senior management and the Board, should ensure that any new risks being introduced are identified, can be satisfactorily controlled and adequately monitored and managed. RM will ensure that the RMP is updated to include how any new risks will be managed and will assist the business in the implementation of additional KRI/KPI as may be needed.

5. Due Diligence for Delegates

The ManCo may wish to make reference to the paper "Guidelines for the Risk Monitoring of Functions Outsourced/Delegated By a Management Company or Investment Company" which has been produced by the ALFI Technical Committee.

As stated above, CSSF Circular 12/546 (clause 7.1.4) requires that "every use of an external service provider must be preceded by written due diligence by the management company on the provider.
In the context of this requirement of diligence, the management company must, amongst others, identify the operational risks deriving from this delegation". It is recommended to extend operational risk management tools to delegated functions to the extent possible .

6. Risk Event Database (RED)

The Risk Event Database is a repository where all information relating to operational errors, including "near misses", fines or other financial gains or losses is stored. The ManCo can define the level and amount of information required for each entry and may wish to consider retaining sufficient data to perform trend analysis and identify departments or processes requiring remediation.

An example of the information recorded would include, but not be limited to:

- Name of Department causing the error/ Name of impacted Department;
- Date the event occurred and date it was discovered;
- Summary and detailed description of the event;
- Root cause of the event and key control failures;
- Concerned procedure (was a procedure missing or incomplete/unclear);

- Remedial action plans (immediate corrective measures and preventative measures);
- Amount of financial impact (actual or potential loss) and the potential to reclaim from a third party/delegate;
- Type of financial impact (timing or economic);
- Status of the recorded event (is it under investigation, awaiting an approval, closed).

The RED may also be used to track all audit findings, both Internal and External Audit, in order to provide an overview of outstanding control issues linked to operational processes, mitigation and follow up status.

RM and senior management should use the RED as one of the tools to assess the overall effectiveness of the internal control structure within the business and to identify where management should be focusing on strengthening processes. The methodology used for the interpretation and quantification of the results provided by the RED shall be defined by each ManCo.

7. Additional tools

A ManCo which is part of a larger financial group and subject to a consolidation under an investment firm may have to conduct the Internal Capital Adequacy Assessment Process (ICAAP) and could use this assessment of capital adequacy based upon the risk profile of their business as an additional tool to facilitate risk assessment. The framework could provide useful guidance with respect to impact of operational errors to the financial and overall health of the ManCo. Monetary losses recorded and assessed could help to identify new risk patterns. The operational errors recorded are used for a scenario analysis to ensure adequate capital reserves are maintained now and for following business years.

Post implementation reviews should be conducted following the introduction of new operational risks into the business in the form of; new funds, systems, procedures, etc. The purpose of such a review being to check if the anticipated control enhancements, implemented to mitigate the new risk, are operating as anticipated.

VI. general principles on the effective reporting of risk management issues to senior management and the board

Adequate risk reporting is integral part of a RM function and in particular for the senior management of a ManCo to ensure they can comply with their obligations and responsibilities of oversight. In order to ensure that the RM function obtain the necessary information from other departments as well as from outsourcing partners, a structured bottom up reporting is needed. Based on the information received and the analysis performed by the (risk) department(s) a meaningful reporting to the senior management and/or a Senior Risk Committee is key to making risks transparent as well to propose and finally decide on mitigating measures.

In the case of operational risk events it is often important that prompt escalation and corrective action is taken to avoid the initial error potentially becoming more significant and perhaps impacting additional funds. For example an error that results in a market exposure should ideally be closed on the same business day that it occurs in order to avoid carrying an overnight risk. The Risk policy and procedures should therefore clearly document how risk events are to be treated and the steps to be followed in the case of a risk event. This document should include a clear escalation timeline and hierarchy of escalation. This document can be summarised as an escalation matrix, as in the non-exhaustive example below:

Escalation Matrix	Who do you call	When do you call
AML Issues	Money Laundering Reporting Officer	Upon identification
Client Complaints	Client Service and Operation Managers	Within 24 hours of receipt
Data Breach	Data Privacy Officer	Upon identification
Error, Fines or Losses	Senior Management/Compliance	Upon identification
Ethics Violations	Senior Management/Compliance	Upon identification
Fraud or Fraud Attempts	Security Team	Upon identification
Technology Failures	Technology Hotline	Upon identification

Error Escalation reporting – The ManCo should consider the use of a standard template to be used to document and escalate any risk event. The information in the report should include:

- Name of department that caused the event;
- Name of impacted parties, type and amount of impact;
- Date the event occurred and date it was discovered;
- Event summary and detailed timeline that describes the event and identifies control gaps or failures;
- Remedial action plans for each control gap or failure;
- Amount of financial impact.

In addition to timely reporting of operational risk events as they occur, or are identified, all operational risks should be recorded in the Risk Event Database (see above) and included in the regular reporting to senior management and the Board.

The "Best Practice Proposals for the Organisation of the Risk Function of a UCITS Management Company or UCITS Investment Company" paper, mentioned above provides more information on risk reporting but in summary the following reporting requirements should be considered:

- The senior management/Board will receive a holistic report on all relevant risk types aggregated. This report will be based on the data gathered bottom up by risk function/senior management;
- The Head of Risk Management/senior management is responsible to receive necessary bottom up reports from relevant departments and/or delegates;
- The Head of Risk Management/senior management will report at least quarterly to the Board of the ManCo;
- The Head of Risk Management/senior management will ensure that Risk Reports are holistic (considering all risk categories identified), timely and accurate;

- The Risk reports will give information on current/new risks including a statement on severity (e.g. low, medium, high) and its evolution over time and measures to mitigate existing risks where possible;
- The Risk Reports must provide the Board with all necessary information to decide on appropriate measures to be taken to control and mitigate all relevant risks;
- The Head of Risk Management/senior management must ensure that any relevant new risk issues deemed to be high will be reported ad hoc to the Board;
- The Head of Risk Management/senior management will oversee that entities report in a timely, accurate and clear manner and are consistent with the framework set by the risk function.

Appendix

appendix I - key risk indicators for operational risk

* None exhaustive table / Not all KPIs may fit every individual company set up

Business Line	Process	Risk	KRI	Category
Corporate level/Structure				
	Employment practices and workplace safety (HR/Facility Management)	• Impact of compensation, benefit, discrimination and termination issues; • General liability (slip and fall etc).	Number of pending lawsuits/claims against company Number of potential lawsuits/claims against company Monetary value of pending/potential items	People People People
	Facility Management/HR	Natural disaster losses Human losses from external sources	Historic figures vs. actual figures Specific patterns of events	Process Process
	Business disruption and system failures	Breakdown of business/communication or production process	Number of system failures identified and resolved Recurrence of specific failures Severity of IT issues	System Process System
	All (Fraud Risk)	Risk of noncompliant bribes/kick backs Hacking damage/ Theft of information Theft/Fraud/ Forgery	Number of hacking attempts/cases Monetary value of losses from Hacking activities Number of events/ number of fraud attempts Monetary losses from events	People System System Process Process

Business Line	Process	Risk	KRI	Category
	Outsourcing (Oversight)	Failure to perform oversight responsibilities for outsourced functions	Turnover of the employees	Process
			Press coverage	Process
			Profit/loss figures	Process
			Investments realised/Budget dedicated to projects	Process
Investment Management				
	Portfolio Analysis	Violation of Ethical standards (Insider Dealing, Market Abuse)	Number of violations	Process
		Conflict of Interest	Number of Conflicts Logged/Approval obtained	People
	Investment decision	Breach of regulatory and other mandatory guidelines	Number of active breaches	People
			Monetary impact of breaches	Process
			Number of passive breaches	Process
		Disputes over performance of advisory activities	Number of complaints and value of claims	People
	Disclosure of information to clients	Unequal/Unfair treatment of clients	Number breaches of disclosure rules	Process
	Risk Management	Breakdown of controls performed	Number of controls not executed	Process

Business Line	Process	Risk	KRI	Category
		Administration		
Transfer Agent	Client Order	Incomplete Application AML/KYC	Number of accounts with incomplete KYC	Process
		Late trading	Number of exceptions from standard cut off times	Process
		Market Timing	Number of suspicious transactions (monetary amount)	Process
		Incorrect processing (manual errors)	Number of revised trades	Process
			Monetary impact of revised trades	Process
		Incorrect/Incomplete Registration details	Number of dormant accounts	Process
			Number of accounts with missing legal documentation	Process
	Electronic Dealing	IT Risk (SWIFT)	Number of incorrect/revised electronic trades	System
	Reconciliations/collection accounts	Accounts are not accurate	Material items > X days old	Process
		Unsettled Subscriptions	Number of unsettled Subs > X days	Process
		Returned Redemptions	Number of returned transactions	Process
			Monetary Value of returned transactions	Process

Business Line	Process	Risk	KRI	Category
	Cash Flow reporting to Portfolio Manager	Material Overdrafts/Activ breaches	Number/amount of Overdrafts	Process
			Number of days target times not met	Process
		Reporting is late or inaccurate	Number of days corrections required	Process
	Contract Notes/ Client reporting	Client complaints	Number of Complaints received	People
			Number of late submissions	Process
	Commission payments	Incorrect payments to distributors	Number of payments reissued	Process
	Client payments	Claims from clients	Losses from incorrect payments	Process
	All	Data privacy	Number of breaches reported	Process
			Number of complaints linked to Data Privacy	Process
	All	Fraud	Number of events occurred	People
			Number of events prevented	People
			Monetary impact of fraud cases	People
Investment Operations	Security Pricing	Use of Stale Prices	Prices unchanged > X days	Process
		Breakdown of external price feed	Number of such events	Process
		Incorrect feed from external vendors	Number of such events	Process
		Illiquid/Unquoted Securities	Number of illiquid positions	Process

Business Line	Process	Risk	KRI	Category
Administration				
			Share write off's	Process
			Number of defaulted securities	Process
			Monetary Impact of write off/defaults	Process
		Broker provided prices		Process
	Trading	Trades place incorrect in System	Number of revised/ failed trades	System
			Financial loss on trades	System
		Use of non-approved counterparties	Number of deviations from Counterparty list	Process
		Breach of Best Execution Policy	Number of complaints	Process
			Number of exceptions reported	Process
	Settlement	Incorrect Settlement of trades	Financial loss from incorrect settlements	System
		Backlog of trade reconciliation	Settlements O/S > X days	Process
	Corporate actions	Accounts not accurate	Number of O/S dividend payments	Process
	Asset reconciliation	Accounts not accurate	Number of Material items O/S > X days	Process
			Monetary value of O/S items	Process
	Collateral Management	Collateral Management failure	Number of incorrect booking entries	Process

Business Line	Process	Risk	KRI	Category
	Fee calculation	Incorrect set up of performance fee calculation model	Number of revised Fee statements	Process
			Fee accrual errors	
Fund Accounting	NAV Calculation	Financial/reputation risk arising from material NAV errors	Number of NAV Material NAV errors	Process
			Monetary Impact of errors	Process
		Frequent immaterial NAV errors	Number of NAV errors <1%	Process
		Incorrect application of Swing Pricing	Number of recalculated NAVs	Process
	NAV release process	Risk of incorrect/ late price release	Number of incidents	Process
	Tax Reporting	Submission of incorrect figures/claims	Number of calculation/submission errors	Process
			Monetary impact of reporting errors	Process
	Safeguerding of assets		Number of subcustodians	Process
			Appointment of new subcustodians	Process
			% of assets transferred to subcustodian	Process
			% of assets not held with the main custodian	Process

Business Line	Process	Risk	KRI	Category
Distribution				
Marketing	Preparation of Marketing Material	Misinformation of current/prospect clients	Number of client complaints	Process
		Errors in translations	Number of errors identified post internal reviews	Process
		Incorrect Factsheets	Number of errors identified post internal reviews	Process
		Failure to comply with local regulations	Number and monetary impact of compliance breaches	Process
Sales	Distributor On Boarding	Inadequate due diligence	Number of accounts affected	Process
		Incomplete AML/ KYC	Number of accounts affected	Process
		Missing legal agreements	Number of accounts affected	Process
	Client on boarding	Misselling of products/services	Number of serious clients complaints	Process
		Incorrect set up of electronic controls for client orders	Number of incorrect transactions not suitable for the client/Losses from correction	System
		Incomplete Legal documents	Number of accounts affected	Process
		Incomplete AML/ KYC	Number of accounts affected	Process
		Client permissions/ disclaimers missing	Number of cases identified	Process

Glossary of terms

AML	Anti-Money Laundering
Board of Directors	Supervisory Function as defined below
BCP	Business Continuity Plan/ Process
Client	Any natural or legal person, or any other undertaking including a UCITS, to whom a ManCo provides a service of collective portfolio management or services pursuant to Article 101, paragraph (2) of the 2010 Law
Compliance Officer	Person who's effectively responsible on a day to day basis for carrying out the services and activities within the meaning of Article 11 of the Regulation No. 10-4
Conducting Officer	Member of Senior Management as defined below
Counterparty Risk	Risk of loss for the UCITS resulting from the fact that the counterparty to a transaction may default on its obligations prior to the final settlement of the transaction's cash flow
CSSF	*Commission de Surveillance du Secteur Financier*, the Luxembourg supervisory authority of the financial sector
CSSF Circular 12/546	CSSF Circular of 24 October 2012 relating to authorisation and organisation of the Luxembourg management companies subject to Chapter 15 of the Law of 17 December 2010 on undertakings for collective investment as well as to investment companies which have not designated a management company within the meaning of Article 27 of the Law of 17 December 2010 on undertakings for collective investment
ESMA	European Securities and Market Authority
EU	European Union
External Service Provider	Any entity to whom the ManCo and Self-Managed SICAV has delegated one or more functions, even if this entity belongs to the same group as the group of the ManCo or of the initiator's Self-Managed SICAV
Fund	• (i) any UCITS or UCI managed by a ManCo or • (ii) a Self-Managed SICAV
Initiator	Entity that has taken the initiative to launch a Fund in Luxembourg
IM	Investment Management
KPI	Key Performance Indicator
KRI	Key Risk Indicator

KYC	Know Your Costumer
2010 Law	Law of 17 December 2010 concerning undertakings for collective investment and implementing Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS)
Liquidity Risk	Risk that a position in the UCITS' portfolio cannot be sold, liquidated or closed at limited cost in an adequately short time frame and that the ability of the UCITS to comply at any time with Article 11, paragraph (2) and Article 28, paragraph (1), point b) of the Law of 17 December 2010 concerning undertakings for collective investment is thereby compromised
ManCo	Management Company means a management company authorised and subject to chapter 15 of the 2010 Law; or self managed company
Market Risk	Risk of loss for the UCITS resulting from fluctuation in the market value of positions in the UCITS' portfolio attributable to changes in market variables, such as interest rates, foreign exchange rates, equity and commodity prices or an issuer's creditworthiness
NAV	Net Asset Value
Operational Risk	Risk of loss for the UCITS resulting from inadequate internal processes and failures in relation to people and systems of the management company or from external events, and includes legal and documentation risk and risk resulting from the trading, settlement and valuation procedures operated on behalf of the UCITS
Proportionality	Principle pursuant to which the senior management needs to assess on a case by case basis the relevant human and technical resources - appropriate to the size and the organisation of the ManCo, and to the nature, scale and complexity of its activities
Regulation No.10-4	CSSF Regulation No.10-4 transposing Commission Directive 2010/43/EU of 1 July 2010 implementing Directive 2009/65/EC of the European Parliament and of the Council as regards organisational requirements, conflicts of interest, conduct of business, risk management and the content of the agreement between a depositary and a management company, as amended

Reputational Risk	Risk of damaging an entity's trustworthiness in the marketplace, i.e. the impact of specific events that could worsen or negatively affect the perception of an entity
Risk Appetite	Amount of risk exposure (e.g. expressed as monetary), or potential adverse impact from an event, that a ManCo is willing to accept/retain
Risk Management Officer	Person who's effectively responsible on a day to day basis for carrying out the services and activities within the meaning of Article 13 of the Regulation No.10-4
RM	Risk Management
RMP	Risk Management Process
Self-Managed SICAV	SICAV established under Part I of the 2010 Law which has not designated a ManCo, within the meaning of Article 27 of the 2010 Law
Senior Management	Persons who effectively conduct the business of a ManCo in accordance with Article 102, paragraph (1), point c) of the 2010 Law in other terms "Conducting Officer"
SICAV	*Société d'investissement à capital variable* (investment company with variable capital)
Supervisory Function	Relevant persons or body or bodies responsible for the supervision of its senior management and for the assessment and periodical review of the adequacy and effectiveness of the risk management process and of the policies, arrangements and procedures put in place to comply with the legal and regulatory obligations, including but not limited with the 2010 Law
UCITS	Undertakings for collective investment in transferable securities, subject to Part I of the 2010 Law
UCITS Directive	Council Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS)
Unitholder	Any natural or legal person holding one or more units/shares in a Fund

alfi
luxembourg
fund industry

The Association of the Luxembourg Fund Industry (ALFI), the representative body for the Luxembourg investment fund community, was founded in 1988. Today it represents more than 1 300 Luxembourg-domiciled investment funds, asset management companies and a wide variety of service providers including depositary banks, fund administrators, transfer agents, distributors, law firms, consultants, tax advisers, auditors and accountants, specialist IT providers and communications agencies.

Luxembourg is the largest fund domicile in Europe and its investment fund industry is a worldwide leader in cross-border fund distribution. Luxembourg-domiciled investment structures are distributed in more than 50 countries around the globe, with a particular focus on Europe, Asia, Latin America and the Middle East.

ALFI defines its mission as to "Lead industry efforts to make Luxembourg the most attractive international centre".

Its main objectives are to:

Help members capitalise on industry trends

ALFI's many technical committees and working groups constantly review and analyse developments worldwide, as well as legal and regulatory changes in Luxembourg, the EU and beyond, to identify threats and opportunities for the Luxembourg fund industry.

Shape regulation

An up-to-date, innovative legal and fiscal environment is critical to defend and improve Luxembourg's competitive position as a centre for the domiciliation, administration and distribution of investment funds. Strong relationships with regulatory authorities, the government and the legislative body enable ALFI to make an effective contribution to decision-making through relevant input for changes to the regulatory framework, implementation of European directives and regulation of new products or services.

Foster dedication to professional standards, integrity and quality

Investor trust is essential for success in collective investment services and ALFI thus does all it can to promote high professional standards, quality products and services, and integrity. Action in this area includes organising training at all levels, defining codes of conduct, transparency and good corporate governance, and supporting initiatives to combat money laundering.

Promote the Luxembourg investment fund industry

ALFI actively promotes the Luxembourg investment fund industry, its products and its services. It represents the sector in financial and in economic missions organised by the Luxembourg government around the world and takes an active part in meetings of the global fund industry.

ALFI is an active member of the European Fund and Asset Management Association, of the European Federation for Retirement and of the International Investment Funds Association.

To keep up to date with all the news from the association and the fund industry in Luxembourg, join us on LinkedIn (The Luxembourg Fund Industry Group by ALFI), Twitter (@ALFIfunds), Youtube, Vimeo or visit our website at www.alfi.lu.

April 2014

For any further information about this brochure or risk management address your requests to the following e-mail adress: alexander.fischer@alfi.lu

Operational Risk Management within UCITS

guidelines