RFM Dr. Imfeld
Risiko- und Finanzmanagement

RODEX RISK ADVISERS
Analytics. Transparency. Management.

Operational Risk Management in Practice: Implementation,

Success Factors and Pitfalls

Efficient implementation for midsize and small Asset Managers, Hedge Funds, Private Equity Funds, Family Offices

Working Paper, Version 1.1, 4 October 2011

Authors:

Dr. Claus Huber, CEFA, CFA, FRM
Rodex Risk Advisers LLC

claus.huber(at)rodexrisk.com
Tel. +41 (0)43 539 76 22

Dr. Daniel Imfeld
RFM Dr. Imfeld, Risiko- und Finanzmanagement
daniel.imfeld(at)rfm-imfeld.ch
Tel. +41 (0)41 761 18 92

Contents

1) Introduction 2

2) How to add value with Enterprise and Operational Risk Management 4

3) A process-driven approach for practical management of operational risk 6

4) Systematic OpRisk process 10

Step 1: Risk Identification 11

Step 2: Risk Mitigation and Control System 13

Step 3: Risk Controlling and Reporting 16

Step 4: Risk strategy, integration with market and credit risk 17

5) Success factors and Pitfalls 18

References 20

1) INTRODUCTION

According to the often-cited CapCo study (2003) about hedge fund failures, 50% of those failures were driven by Operational Risk. Operational risk management is increasingly important - not only for hedge funds, but also for other asset management companies – such as private equity companies, family offices or independent asset managers. Pressure from investors and regulators as well as increasing market competition require state of the art operational risk management from these institutions. In this article, we focus on Operational Risk Management for mid-sized Asset Management companies which are not part of a large international banking organisation and hence will not have fully developed staff departments for Operational Risk, Compliance or Internal Control. Many of these functions in mid to smaller size asset management organisations will be part-time activities of several people. With regard to Operational Risk, these mid size asset managers face many specific challenges like:

- Large asset base under management, but a small number of employees. The financial assets are comparable to large industrial corporations with several thousand employees.
- Segregation of duties in such small organisations is difficult.
- Increasing regulatory focus and burden.
- Creative business environment for portfolio managers and product structurers.
- Often young organisations with no tradition of risk and control management or structured processes.

We take a practitioner's view of how an operational risk framework can be implemented as part of an enterprise wide Risk and Control system in a "hands-on" approach. We outline how a mid-sized asset management organisation can develop systematically an integrated perspective on its main risks and set priorities on how to mitigate and control these risks.

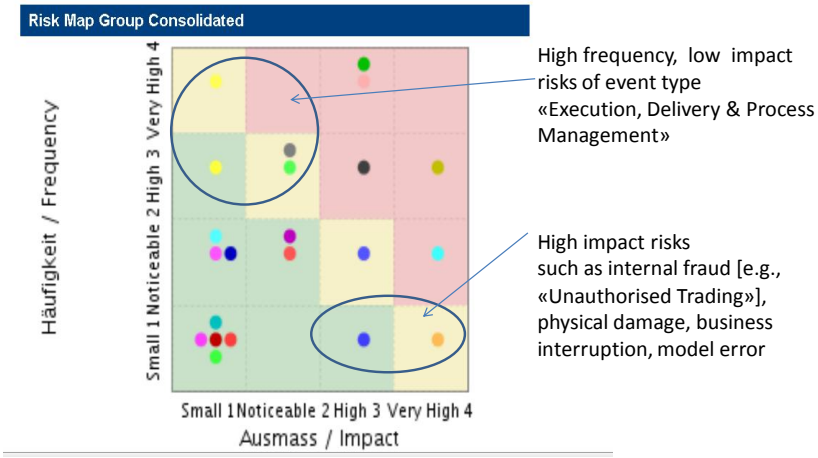


Figure 1: Risk Map Source: SME Risk Platform: RFM Dr. Imfeld, Acons Governance&Audit AG, Avanon AG

A pragmatic instrument supporting such an integrated risk perspective is a loss severity (impact)/ loss likelihood (frequency) matrix or Risk Map as illustrated in Figure 1. It provides an overview for all risks analysed on the company level, each bullet representing the expert assessment result of an identified risk scenario.[1] Large risks are shown in the upper right red zone, smaller risks in the lower left green zone. High frequency but low impact risks often related to a process or quality issues are shown on the upper left corner, whereas rare but catastrophic risk scenarios are plotted on the lower right corner.

Many companies still view (operational) risk management only as a regulatory burden and a cost factor. Yet, practical experience shows that companies profit from Operational Risk Management provided that they design and practice it as a management instrument. It then helps to achieve company goals, create competitive advantages and improve business efficiency. These companies will normally have no problems complying with regulatory requirements. However, in companies that only look for the regulatory minimum and have little interest in how to implement operational risk for the benefit of their company, operational risk management deteriorates into a costly paper exercise. Only a true integration of the Risk and Control System as part of an entrepreneurial management system will contribute to the survival and long-term success of an enterprise.

How can Operational Risk Management within an asset management company as part of an Enterprise Risk Management framework look like? We answer this question in four parts:

- A short overview on the terms used and how risk management needs to be designed to add value [section 2].
- An illustration of key operational risks based on a generic process model for asset management activities [section 3].
- An outline of the key steps in a systematic operational risk management process illustrated for one specific risk scenario. We show how a structured risk identification and documentation works, how mitigation measures and controls for the risk can be implemented, tracked systematically and how continuous reporting allows follow ups on the status of risks and action plans [section 4].
- In summary, we highlight typical success factors and pitfalls in the implementation from the concept phase to the implementation of an IT-supported Risk Management process [section 5].

[1] Companies with more experience in Operational Risk Management may use a multi scenario approach for each risk event, differing for example between an expected standard case and a worst case per risk event.

2) How to add value with Enterprise and Operational Risk Management

In the financial services industry, an important source of failures in Risk Management is the silo approach to market, credit and operational risk. The silo mentality results in a lack of understanding of operational risk management and internal controls as an integral part of the Enterprise Wide Risk and Control Management System. Since many functions in the organisation such as Asset Liability Management, Operational Risk, Internal Control, Internal Audit, Security and Business Continuity Management and Compliance are all involved in risk management activities, it is very important to set up an integrated risk and control framework based on one risk policy.

To start with, a risk policy should be defined as a short (1-3 pages), constitutional document in easy-to-understand-language. Ideally, the policy covers all types of risks at the top level with Operational Risk as one important category, but including market, credit and core business or strategic risks. The policy describes the main principles for how the organisation manages its risks and briefly mentions key elements of the Risk Management framework to be set in place. Besides the Risk Policy itself the key elements of the Risk Management Framework are the Risk Management Process, Roles and Responsibility, Organisation, Methods and Instruments, IT-Solution, Risk Communication. Over time (and it will take years rather than months) the integrated Risk Management Framework will encourage responsible functions in the organisation to develop a common enterprise-wide understanding of risks as a basis for better business decisions. In addition, line management will be less disrupted by differing concepts, terms or repeating workshops about ultimately the same thing, namely the risks the company has to manage.

A starting point of each risk management activity is the identification of potential risks and an assessment of their relative importance for the organisation. Which risks may endanger the success of the company and the achievement of the company goals? Only on the basis of an integrated risk perspective, as illustrated in the Risk Map in Figure 1, the board and management are able to prioritise key risks and to prepare effective risk mitigation plans to keep the risks within acceptable limits of the company’s risk appetite.

A value added strategy on the basis of an enterprise wide risk perspective will help to:

- Prioritise and focus on key risks and risk combinations that may endanger the company goals and mitigate them with efficient, company-wide mitigation measures and controls,
- save costs by avoiding unnecessary hedging, insurance or security measures, or by reducing the number of unnecessary controls for risks with only negligent impact,
- improve process quality through better understanding of risks in all processes,
- enhance the understanding of dependencies and correlations between different operational risks but also between operational risks on one side and market, credit or core business risks on the other side,

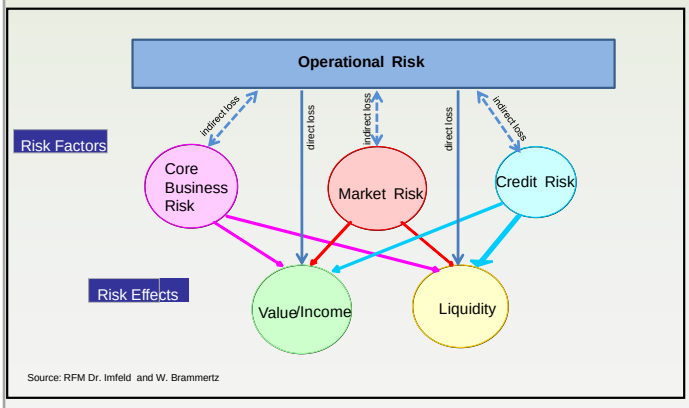
- Assure adequate, but realistic crisis management and business continuity measures that will allow the survival of the business in critical periods. Often simple measures can have a dramatic (positive) impact.
- Ring-fence operational risks to avoid surprises and simultaneously adding value by consciously allowing investing more risk capital for the core business and wanted market or credit risk.
- Assure compliance with regulations.

What is Operational Risk?

We define this by describing possible risk events leading to an *actual* outcome(s) of a business process to differ from the *expected or targeted* outcome(s). These events can be due to inadequate or failed processes, people and systems, or to external facts or circumstances (see also references at the end of the article under Basle II or ORX documents).

In this context it is key to understand that operational risks are often the cause and driver of credit, market and core business or strategic risks. This means that operational risk events can have a direct or indirect impact on the value / earnings of the company or the liquidity available. For example, a direct effect of a burglary in the company building could lead to losses of stolen computer equipment. Indirect effects via market, credit or core business risks often are more severe than the direct impact if, for example, confidential data were stored on the stolen computers that subsequently get published on the internet. In rare cases such as extreme market or credit risk volatility, one could also argue that market and credit risk may be causing unexpected operational risk events because of a breakdown of the standard processes in such a period.

Overview: Operational risks can cause direct losses or indirect losses via market, credit or core business risk



Op Risk Events risk scenarios: what can go wrong
Changing the investment style of the fund without the approval of investors [style drift].
Error in risk model: For example, wrong duration for a High Yield bond
Non-consideration of credit risk from complex, badly documented structured product
Funding Liquidity: Large investor(s) withdraw money, forcing shut down of the asset manager
Data error in base line scenario for market data
Unauthorised trading & style breaches, breach of investment guidelines
Material misstatement of asset values
[Fraudulent] misrepresentation of fund performance [in particular hard-to-value assets]
Not meeting deadline and quality requirements
Wrong data access rights to salary system attributed to employees
Failure to supply of key outsourcing provider, not meeting SLA requirements.

Figure 2: “What is Operational Risk?”

3) A PROCESS-DRIVEN APPROACH FOR PRACTICAL MANAGEMENT OF OPERATIONAL RISK

Our goal is to develop systematically a full picture of the operational risks the organisation is facing. The following two conceptual elements will assure that we can cover the whole risk universe.

1. A clear risk concept and a categorisation that covers all operational risks.

2. An End-to-End basic process model for the key processes in the organisation

Risk concept and categorisation: The first important structural element in the operational risk management framework is a clear risk concept with ideally an enterprise-wide categorisation of risks. To this end, a company specific risk framework is beneficial. The "event, cause and effect"-type risk categorisation concept based on Basle II[2] or the ORX[3] can provide helpful guidance as a template and first step towards a company-specific risk categorisation. In Figure 3 the basic idea for risk categorisation is illustrated. The main category in the middle structures possible risk events that describe what can go wrong. Each event can have one or more causes and several impact types. Typical cause type structures are the often used categories People, Process, Systems, External Causes.

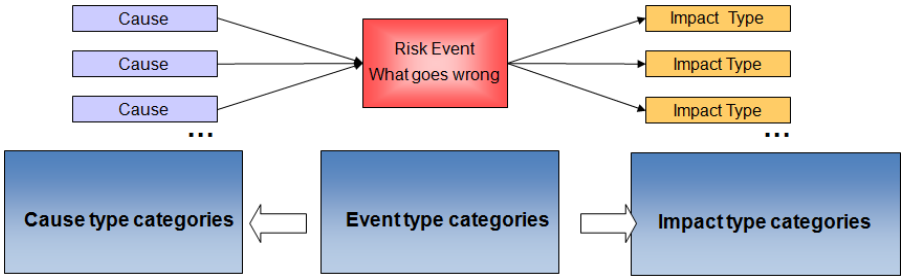


Figure 4: Event / Cause / Impact risk categorization

How could this risk categorisation be applied in practice? Let's look at the example of unauthorised trading. History has seen several high profile breaches of investment guidelines and limits. One of the most prominent examples of the recent past was the unauthorised trading by Jerome Kerviel, which led to a loss of EUR 4.9 bn at his employer, Société Generale, in 2008. In September 2011, UBS lost USD 2.3 bn because of unauthorised trading of one of its employees, Kweku Adoboli. This risk is usually not frequent in occurrence, but it may have a huge impact on market or credit risk and hence it is a rare, but critical event. The risk *event* "Unauthorised Trading" is *caused* by people trading beyond their limits, which is possible because of insufficient controls and processes. *Impacts* can be, for example, unwanted market risk due to large positions, fines imposed by the regulator, and a damaged reputation because of headline risk.

The official categorisations of Basle II or ORX can provide guidance for defining company-specific operational risk categories. The categorisation helps 1) to avoid confusion about risk causes, risk events and the impact of a risk and 2) it allows to group similar risks from the same risk event category and supports a more efficient design of mitigation measures for similar risk events or risks with the same cause. Table 1 below gives an overview on operational risk loss events by the Basle II main risk event type categories. It shows that process failures cause the largest amount of operational

[2] Cf. Bank for International Settlements (2001), p. 19.
[3] Cf. ORX Operational Risk Reporting Standards (2011).

losses for asset managers [53%], followed by Clients, Products & Business Practices [31%] and Internal Fraud [11%]. The latter includes, for example, unauthorised trading.

	Internal Fraud	External Fraud	Employment Practices & Workplace Safety	Clients, Products & Business Practices	Damage to Physical Assets	Business Disruption & System Failures	Execution, Delivery & Process Management	All
in EUR millions	27	2	6	75	1	4	128	243
in %	11%	1%	3%	31%	0%	1%	53%	100%

Table 2: Distribution of annualised loss amounts by event type for asset management units of banks

Process model: The second conceptual element assuring a full picture of all risks is a basic process model. An end-to-end perspective on how different processes function together in the asset management organisation and an understanding of critical process interfaces is a good starting point for systematic and successful risk identification. All risks identified are allocated to a specific process and an organisational unit in order to assure clear ownership in the line management for specific risks. Large organisations often maintain fully developed process models in a specialised process management department.[4] For smaller or midsize organisations, the operational risk and control management does not require a costly process modelling infrastructure, but a generic process model with a clear end-to-end perspective can help to systematically identify risks.

In Table 3 we illustrate an example of a generic process model for an asset management company. For illustration purposes we list typical risk scenarios for each process and describe briefly for each one the actual risk event, the cause of the event and possible impacts. Take for example the event “Unauthorised trading & style breaches, breach of investment guidelines”. The risk will mostly occur in the process “Asset Management, Portfolio Management”, which belongs to the Core Business Processes in Table 3.

[4] For an overview of those models, see, for example, van der Aalst et al. (2000).

Table 3: Op Risk Events by process (source: RFM Dr. Imfeld, Rodex Risk Advisers)

	Process Name 1st Level	Process Name 2nd Level	Op Risk Events risk scenarios: what can go wrong	Impact	Cause
Management Processes	Strategy and business Planning	Strategy process	Changing the investment style of the fund without the approval of investors [style drift].	Drift to area of non-core expertise. Investors redeeming, additional market and credit risk,	People , Guidelines
	Risk Management Internal Control	ORM, Internal Control, Compliance	No centralised database or only fragmented data about Operational Risk available	Recurring Op. Risk incidents causing losses and binding resources	Inadequate systems to deal with Operational Risk
		Market Risk	1) Error in risk model: For example, wrong duration for a High Yield bond	Portfolio overhedged, unwanted P/L	People, Processes, Systems
			2) System Breakdown	Portfolio manager is left without reliable sensitivities ["flying blind"]	system, datafeeds
		Credit / Counterparty Risk	1) Non-consideration of credit risk from complex, badly documented structured product	Wrong estimate of credit risk exposure, higher credit risk than realised	Bad maintenance of excel based documentation, data not in standrd system.
			2) Wrong calculation of credit risk exposure, exceeding credit risk limits on concolidated group basis	Wrong estimate of credit risk exposure, higher credit risk than realised	Old, not up to date counterparty data for group structures of counterparties
			3) Access to liquidity impeded, forced liquidation	Margin requirements in- creased due to market vola-tility, credit lines frozen, liqui-dity mgmt. not prepared	Prime Broker going bankrupt, Market volatility
		Liquidity Risk	1) Asset Liquidity: For example, low market liquidity not adequately reflected in risk tools, thereby understimating Value at Risk	Risk figures underestimating actual risk	Inadequate systems to reflect liquidity risk, people
			2) Funding Liquidity: Large investor(s) withdraw money, forcing shut down of the asset manager if investor base is not diversified	Fund being forced to liquidate because of redemptions	narrow investor base
		Risk Integration	Risk figures of different departments and risk categories cannot be aggregated	Risk situation distorted, may lead to wrong business decisions	Different measurement methods in place; time delays and measurement asynchronities
Core Business Processes	Product Development	Product Development	Wrong documentation of risk exposure in the product	Liability law suit for faulty consultig of clients	Process, People
	Sales	Sales	Inappropriate sale oand consulting related to complex products for non-institutional clients	Liability law suit for faulty consultig of clients	Process, People: Lack of training, Badly designed incentive system for
	Asset Management process	Strategic Asset Allocation process	Data error in base line scenario for market data	Portfolio implementation too far away from SAA benchmark	Manual interface based on excel sheets , no auditable data versions
		Portfolio Management	Back log of [derivatives] trades	Market risk	System, people, processes, technology
			Unauthorised trading & style breaches, breach of investment guidelines.	Market risk, sanctions (fine) as a result of non-compliance, damaged reputation	People, insufficient controls and processes
Support Processes	Treasury	Liquidity Management, Hedging etc.	Unwanted market risk exposure inade- quately hedged [for example, wrong FX or interest rate exposures due to complex spreadsheets rather than robust risk tools]	Unintentional P/L impact, unexpected margin calls and cash impact	System, people, process
	Finance / Back office	Accounting , Fund administration and documentation (Transaction capture, P&L/NAV)	Wrong booking of subscriptions / redemptions [for example, subscriptions erroneously added to NAV when calculating performance]	Leading to wrong NAV and over-/ underestimating the performance. Material per-formance restatements can lead to investors losing confidence in processes	People, Processes
			Data processing error. An investor in a PE fund of funds, NAV und unfunded commitments need to be taken from capital account statements, put into the PE FoF's systems, then transfered to the investor's systems in a manual process.	Wrong exposure and P/L figures	People, Processes, systems
		Financial Closing	Material misstatement of asset values	Restatement, loss of reputation, loss of future buisiness	Delay in data delivery, inadequate systems
		Management Reporting	Delayed and incomplete reporting	Wrong assumptions for business decisions, marekt risk	Inappropriate systems
		Reporting to Investors	Fraudulant misrepresentation of fund performance [in particular hard-to-value assets]	Wrong exposure and P/L figures	People, wrong incentive structure
		Regulatory Reporting	Not meeting deadline and quality requirements		
	HR	Recruiting	Inadequate resources for fund strategy(s)	Underperformance	People
		HR Salary	Wrong data access rights to salary system attributed to employees	Sanction, law suit due to non-compliance with privacy laws	People, System
	Procurement	Outsourcing, SLA third parties	Failure to supply of key outsourcing provider , not meeting SLA requirements.	market risk, loss of business	External event, catastrophic event
	IT	IT	Project delay for propriatory software development as a base for new products	Delay of market launch of new product	Process: unrealistic planning, People: lack of resources

Based on the two conceptual elements risk categorisation and process model we make sure to cover the relevant universe of risks in the organisation. A matrix like Table 4 can be used to assign identified risks to one risk category and one process. This matrix is typically the result of a risk workshop, where internal and external experts give their assessments about various operational risks of the company.

Table 4: Matrix for identifying risks by processes and event type category

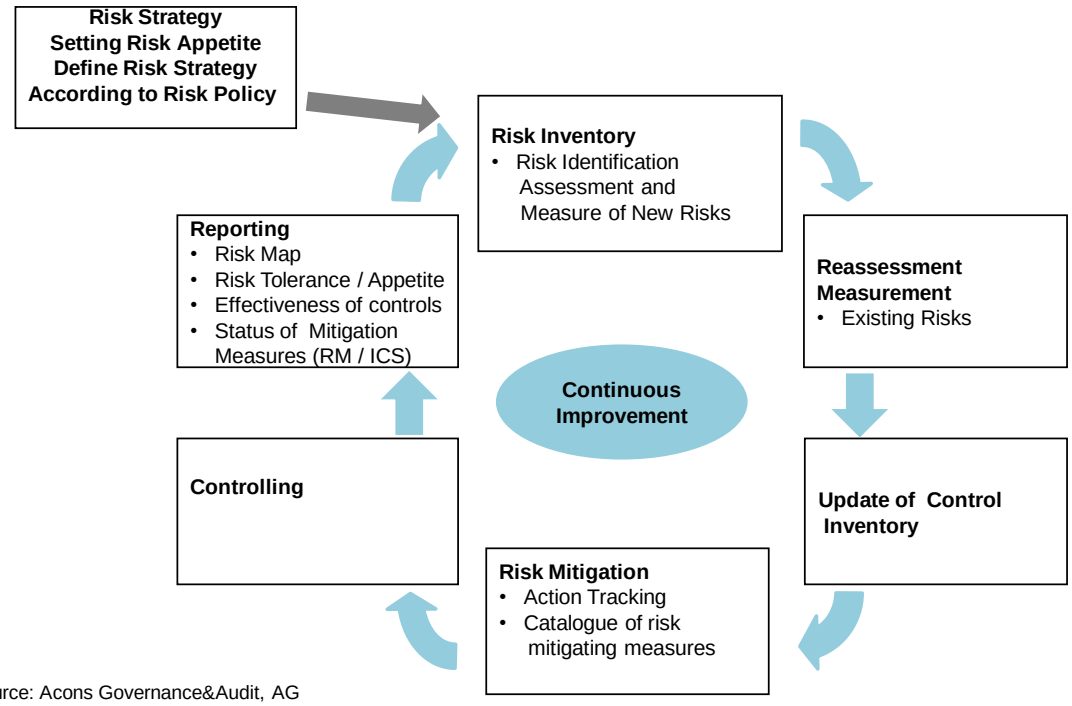
		Event Type Categories						
		Internal Fraud	External Fraud	Employment Practices & Workplace Safety	Clients, Products & Business Practices	Damage to Physical Assets	Business Disruption & System Failures	Execution, Delivery & Process Management
	Process Name 1st Level							
Manage-ment processes	**Strategy process and business planning**				x			
	Risk Management, Internal Control	x			x		x	x
Core Business Processes	**Product Development**				x			x
	Sales		x			x		
	Asset Management process	x			x			x
Support Processes	**Treasury**							
	Finance / Back office			x				
	HR			x				
	Procurement						x	x
	IT							x

Source: RFM Dr. Imfeld / Rodex Risk Advisers

4) SYSTEMATIC OPRISK PROCESS

Based on the example “Fraudulent breach of investment guidelines and investment limits” from our risk list above, we illustrate the systematic risk management process from risk identification and/or risk reassessment to mitigation, controlling, reporting and to finally defining a risk strategy in line with the risk policy (see Figure 5). The illustrations in the tables below show structured documentation for identified risks, mitigation measures and controls. The illustrations are based on anonymised examples recorded on an IT-Operational Risk platform for SME clients.[5] The sample reports show how to systematically gather structured information on risks, keep up with risk mitigation measures and assure that necessary controls are known and performed as expected. The structured information allows straightforward risk analysis and aggregation, simple documentation and reporting on risks, action plans and status level of the control system at any management level required.

Let’s assume our company has defined the risk management framework and outlined it in the risk policy. The operational risk management cycle starts with the first implementation step: Creating the risk inventory by risk identification and risk assessment.



Source: Acons Governance&Audit, AG
RFM Dr. Imfeld

Figure 5: Iterative risk management process

[5] The OpRisk platform is specifically designed for smaller and medium sized companies. The solution was developed in a joint venture of two consulting partners for risk management and internal control (Acons Governance&Audit AG and RFM Dr. Imfeld) and a software solution partner (Avanon AG). The solution is provided on an outsourcing basis (software as a service) and can be combined with content related support on risk management, internal control and internal audit for smaller to medium sized organisations that lack capacity or expertise in their own staff. The conceptual content is owned by the joint venture partners.

STEP 1: RISK IDENTIFICATION

a) Risk Assessment

Typically a workshop including key experts from the different processes is used to identify and collect an initial inventory of relevant operational risk scenarios. The better the risk assessment and the risk information gathered is structured, the more successful will be the future continuing reassessment process [Figure 6].

In our example, the risk scenario “Fraudulent breach of investment guidelines and investment limits” was identified during a risk workshop as part of the process no. 4.1, “Asset Management, Portfolio Management”. A by-product of the risk identification step is that the people in the organisation are forced to think about what can happen, who or what might be the cause for the risks, and how the risks can be mitigated / addressed. In Table 5 we illustrate a minimum of structured information that is collected for each risk scenario in the risk inventory database.

Risk Scenario	
Reference Id	ORSA-20110704-00001
Short Description / Name	Fraudulent exceeding of investment guidelines and investment limits
Description incl. Examples	Portfolio manager engages on purpose in transactions that exceed trading limits and are not in line with investment guidelines. Systematic (intraday) trading outside of limits.
Event Type Category	3. Operational Risks / 3.6 Fraud / Theft
Cause Type	Internal Causes / People Internal Causes / Processes and organisation
Impact Types	Accounting, Profit and Loss & Balance Sheet Financial impact on assets Reputation, Cash Flow, Liquidity
Organisational Unit	/ 99.9 Financial Institution / Company X AM
Process	4. Asset Mgmt. / 4.1 Portfolio Management
Risk Owner	Head Portfolio Management
Contact Person Tool	Test User
Internet Link (http://...)	--
Attachments	0
Status	TMP: temporary
Entry Created At	2011.07.04

Table 6: Structured risk assessment, information stored in the risk inventory

Source: SME Risk Platform by RFM Dr. Imfeld, Acons Governance&Audit AG, Avanon AG

Additional important points in this table are that the risk is made visible to people in the organisation, thereby raising awareness, naming an owner for the risk and clearly assigning responsibilities.
In order to quantify the potential loss in monetary terms [e.g., in USD or EUR], additional information about loss frequency [low, noticeable, high, very high] and loss severity [small, noticeable, critical, catastrophic] is collected, see Table 7. The assessment and quantification are based on expert discussions. Good results for risk evaluation are achieved if unit heads and risk or process experts agree on the valuation of the risk.

Risk Scenario Assessment in terms of impact and frequency	
Please assess the frequency and the Impact/Severity of the risk scenario	
Frequency: **X** low o noticeable o high o very high	
Impact / Severity: o small o noticeable **X**critical o catastrophic	
Is Linked To	
Active Risk mitigation Measures in place or development	
ReferenceId	ORAP-20110704-00003
Object Type	Risk mitigation , Internal Control System
Object Info	Short Description: Four eye principle on PM transaction with size exceeding EUR 1 mio.
	Status: TEMP: Temporary
Added By User	M. Colper
Date	2011.07.04 22:12:17

Table 7: Frequency / severity assessment and risk mitigation methods for the example

Source: SME Risk Platform by RFM Dr. Imfeld, Acons Governance&Audit AG, Avanon AG

The collection of the individual risk scenarios is the starting point of a risk inventory database. It includes also reference links to planned or implemented risk mitigating measures or implemented key controls that help to mitigate the risk [see **Table 7**]. A key control for our example could be to introduce a four eye principle on transactions exceeding EUR 1 million [see step 2 below].

A midsize asset manager may start its risk inventory from the initial risk assessment with three to five risks per process, adding up to 30-50 risk scenarios in the database. Not all of those risks are key risks, but experience shows that it is advantageous not to confine to the top ten risks only. If 30 - 50 risks are reassessed systematically in a certain frequency [for example, annually], chances are high to identify new risk trends. Hence it is recommended to define the top ten list out of 30 - 50 main risks and keep the other risk scenarios documented in the sense of a watch list.

b) Other Risk identification Instruments:

Risk scenario identification is usually the first and simplest method to implement for midsize asset managers. At a later and more advanced stage, the following two methods could be developed:

1. **Loss data collection on actual loss events:** In contrast to potential risk scenarios, we identify operational risks also based on experience by collecting systematically information on past actual loss events. It is useful to learn from own or other organisations' historical risks that materialised in an actual loss or resulted in a "near miss". These methods are widely used in airlines or hospitals, to some degree also in large banks. Typical loss event types that are tracked are:

    - Insured loss events: liability cases with long term impact for many years, property losses, theft, business interruptions with complex multi-dimensional impact,
    - Uninsured loss events such as:
        - customer complaints,

- internal fraud cases,
- Major IT-break downs,
- data entry errors in transactions with market or credit risk impact,
- loss of legal documents,
- law suits with contingent liabilities where actual reserves are marked on the balance sheet

Industry specific loss statistics and loss data bases for operational risks are available from, for example, the Bank for International Settlements, from whose reports the data in Table 2 were taken. Operational Risk Data eXchange [ORX] collects loss events by business segments of large banks. Algorithmics offers a database for financial institutions, covering banks, insurance companies as well as hedge funds.

2. Key risk indicators as an early warning system

Key risk indicators can be another useful method to identify, measure and model operational risks. Similar to early warning signs for key performance indicators or for market, credit or core business risk we look for leading indicators that may serve as early warning signs for operational risks. Typical applications would be:

- IT-related performance indicators for IT-system operations: system errors in transactions,
- Continuous observation of adherence to implemented trading limits,
- Tracking of customer complaints by frequency and topic,
- Number of pending law suits with contingent liabilities,
- Employee turnover by department,
- Indicators for high market volatility and turbulence where operational errors may result in more extreme effects on market and credit risk.

Using key risk indicators as a method for risk identification is usually the case in organisations that have developed a few years of experience with risk assessments and systematic loss data collection. Based on the latter, some key risks might have been identified for which an early warning risk indicator system then can be developed. Assuming a critical risk with fraudulent breach of risk limits was identified based on assessments, key risk indicators analysing intraday limit breaches for trading portfolios could be introduced.

Step 2: Risk Mitigation and Control System

In order to adequately assess the impact of an identified risk on the organisation's business, one has to consider existing controls and mitigating measures that already reduce the likelihood and/or severity of the risk scenario identified. A risk mitigating measure, in contrast to a control, is usually a one-time measure for which an implementation date and a responsible person is defined. In the risk assessment for the example above we have attached summary information on mitigating measures and key controls that are in place and systematically tracked [see **Table 8** and **Table 9**]. How can risk

mitigation and controls be integrated in an operational risk framework? Below we illustrate the structured information that is systematically documented and tracked for risk mitigating activities. A simple workflow support in the IT-solution allows differentiating for each object [risk scenario, mitigation measure, control, loss event] three different statuses and helps to keep track of the implementation steps. Such a work flow support results in improved transparency, efficiency and data integrity compared to the widespread Excel/Word solutions that typically create problems with regard to user access rights, data integrity and confidentiality.

In the simplest workflow we differentiate between:

- a status “Temporary”: Data entry on risks, actions or controls not yet finalised,
- “Active”: The documentation is approved and actions can be implemented and risks can be reported,
- “Completed” or “ready to archive”: Action plans are implemented or risks are being reassessed, therefore the information is kept as an archived data entry.

In our example, the risk mitigation techniques to be introduced are a strict screening process of all individuals who work in portfolio management. The Head of Personnel is responsible for this process [see **Table 8**].

In addition to one time mitigating measures, the **internal control system** will support risk mitigation in systematically reducing identified risks to an acceptable level. For our risk example, a four eye principle is to be implemented for transactions above EUR 1 million as a mitigation technique. The control is, however, not yet effective and needs to be improved, as can be seen in **Table 9** from the entries in the rows “Status” and “Control Assessment”. The risk controller is supposed to follow up on this control and assure a proper implementation. The systematic action and control tracking instrument will allow keeping track of pending optimisations. For example, once per month the responsible person receives an email listing of all “Temp” items.

Mitigation measure	
Reference Id	ORAP-20110704-00001
Type	Action Plan
Type of Mitigation Measure	Risk Management / Strategy
Short Description / Name	Personnel policy and four eye principle for transactions with size > 1 million.
Description of Measures	Introduce strict assessment of individuals to work in portfolio management. Annual Reassessment and documentation as a key control. Introduction of a four eyes principle on transactions with size above EUR 1 million. Document as a key control.
Responsible Organisational Unit	/ Financial Inst./ Company X AM/
Process Allocation	Financial Institution / 4. Asset Mgmt./
Implementation Target Date	2011.12.08
Priority	High
Cost of measure (in local currency) optional	10,000.00
Responsible for Measure	Head of Personnel
Contact Person Tool	Nutzer 2, Test-Demo (Test-Demo)
Status	TEMP: Temporary
Internet Link (http://...)	--
Attachments	0

Table 8: Risk Mitigation Source: SME Risk Platform: RFM Dr. Imfeld / Acons Governance&Audit AG / Avanon AG

Internal Control	
Reference Id	ORAP-20110704-00003
Type	Internal Control System, Financial Reporting Control/Operations Control
Short Description / Name	4 eye principle on PM transaction with size exceeding 1 mio.
Description of Control	Double signature required for transactions in PM exceeding 1 mio. 2nd signature required from employees of same or higher hierarchical level.
Responsible Organisational Unit	/ Financial Inst./ Company X AM/
Risk Description	Fraudulent transaction outside of investment guidelines or investment limits.
Relevance of Control	Key Control
Process Allocation	/ 4. Asset Mgmt. / 4.1 Portfolio Managemnet
Control Frequency	Transactional
Control Automation	Manual
IT-Systems	--
Proof of Control / Evidence	
Control Assessment	To be improved
Responsible for Control	Head of Asset Management
Contact Person Tool	B-Cooper
Status	TEMP: Temporary
Internet Link (http://...)Attachements	--

Table 9: Control Information

Source: SME Risk Platform: RFM Dr. Imfeld / Acons Governance&Audit AG / Avanon AG

Step 3: Risk Controlling and Reporting

The goal of the risk management process is to keep identified risks in line with the risk policy and risk strategy approved by the Board of Directors and the executive team. The risk and control function assures that existing controls are actually performed and newly approved risk mitigating measures are implemented as planned.

How can the information about operational risks be processed, reported and followed in a structured way? An integrated risk and control overview can help to keep an up to date perspective and allow timely reporting on the status of risks, mitigation measures and controls. The Dashboard function shown below (Figure 7) gives an idea of how the risk and control function can make use of the structured information on risk scenarios, loss events, key indicators, controls, and mitigation measures. Relevant information about this is stored in a database. A simple workflow support allows keeping track of data versions of actual current and archived data.

The first part of the dashboard overview [see table “All Risks by Process”] shows all identified operational risks for the asset manager. For illustration purposes, we show only four different risks. A short description of the risk is displayed, together with the risk owner and the status [temporary, valid, archived]. The Risk Map gives a quick assessment along the two dimensions loss frequency and loss impact. Our example risk “Fraudulent breach of investment guidelines and investment limits” shows up in the Risk Map as the yellow point [noticeable frequency / very high impact]. In the middle of the dash board an overview on the status of mitigation measures and the implementation of controls is given. This company has also started a loss data collection effort as part of risk identification and tracks the different operational errors as key risk indicators. On the lower left side core system errors for asset management transactions are tracked as key risk indicators on the basis of percent of transactions that show a system error, where up to one percent is accepted within the benchmark. On the lower right side, reference documentation of individual loss events is listed and is pending for confirmation by the responsible line manager.

The dashboard summary gives an up to date picture on the overall risk situation of the company and supports managers in the actual management of the identified risks. The more developed the risk management approach, the better integrated the risk dash board is in the overall management information system and business planning.

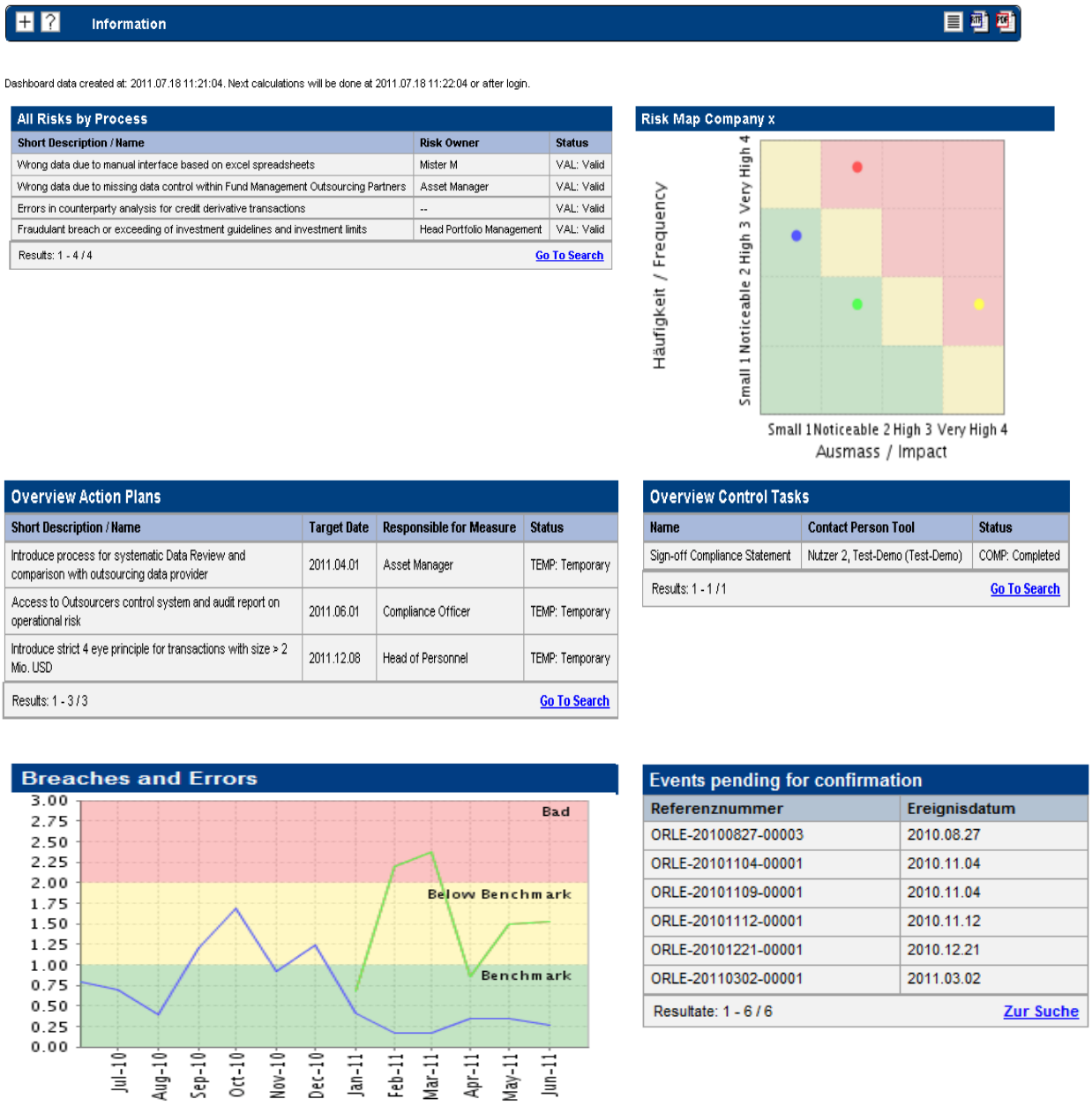


Figure 7 Example personal Dashboard Oprisk Controlling

Source: SME Risk Platform: RFM Dr. Imfeld / Acons Governance&Audit AG / Avanon AG

STEP 4: RISK STRATEGY, INTEGRATION WITH MARKET AND CREDIT RISK

Now the basic steps of the risk management process are performed for our example risk “fraudulent breach of guideline/ limits”. The risk is identified, an action plan and a control are put in place. But is it efficient to manage each risk individually? A practical risk concept allows for aggregation by risk categories and for consolidation across business units. In an initial operational risk concept simple risk aggregation and consolidation methods can be introduced. Grouping risks by categories to look for worst case risk scenarios, consolidating risks across business units and evaluating dependencies, correlation or diversification potential between risks can be introduced already with relatively simple methods and are an important step towards an integrated risk perspective. In an early stage of risk

management for mid-size asset managers it will not be necessary to engage in complex quantitative measurement such as aggregated loss distribution estimation based on monte carlo simulations or risk capital allocation exercises. But it will be worthwhile to evaluate some key “what-if” operational risk scenarios and their impact on market and credit risk in the form of stress scenarios for the integrated risk evaluation of the organisation.

Based on the structured risk information gathered and the integrated perspective on all relevant risks, mitigation measures and implemented controls, the risk manager is able to produce risk reports according to the need of any type of management level. A key function of an integrated risk report is to allow management to understand the whole risk landscape and to set priorities when answering the questions below:

- Which risks need further mitigation and a prioritised action plan with approved budget for implementation since they might endanger specific company goals?
- Which risks can be accepted without further mitigation?
- Where can the company save costs by giving up historically established mitigation measures or controls since the risks are not really threatening company goals? This will allow to save cost in insurance, hedging, unnecessary security measures or to save time by giving up unnecessary control activities.
- Which risks diversify within the organisation? Often risks seem important from one department’s point of view, but for the organisation as a whole the risk is diversified and acceptable.
- Which risks or risk combinations need further analysis and investigation or the development of additional risk evaluation tools like an early warning system, detailed scenario modelling and stress testing or systematic loss tracking?
- Which risks have to be accepted since no further mitigation is possible as long as the company is staying in that business? How should the company communicate to stakeholders about these types of risks? What kind of contingency and business continuity plan has to be prepared for actual incident management if these risk events materialise?

Working through these steps will help to create value based on a systematic risk management framework and move risk management away from a pure cost centre to actual value generation by enabling the company to achieve its goals in the core business strategy.

5) Success factors and Pitfalls

In this final section and as a summary we highlight some success factors and pitfalls that companies experience when implementing operational risk frameworks.

1. A key element for success is to start operational risk management within a **well-defined framework**. Main elements of such a framework are: A clear risk concept (possibly combining risks and chances), a Risk Policy, the Risk Management Process, Roles and Responsibility, Organisation, Methods and Instruments, IT-Solution and Risk Communication.
2. The risk policy should be defined in the beginning as a **short (1-3 pages), constitutional document in easy-to-understand-language**. It describes the main principles how the

organisation manages its risks and very shortly mentions key elements of the framework to be set in place. Ideally, the policy covers all types of risks at the top level. The risk policy should be **approved by the board**. Many companies suffer from different and inconsistent policies for market risk, credit risk, operational risk, internal control, information security etc. A consistent enterprise-wide approach can save a lot of resources at the level of line managers who finally have to manage risks on a daily basis.

3. Ideally **derive the goals for risk management from the company strategy**. Implementation tools could be, for example, a Balanced Scorecard or Economic Value approach. Align interest and incentives of managers to clearly defined goals in the risk management process. Include goals for risk management steps into the individual manager's objectives and assure its relevance for his/her bonus.

4. Set up a systematic risk management process with clearly defined **interfaces to strategy, planning and budgeting processes**. It is too easy to agree on risk mitigation as long as you do not have to pay for it.

5. Define **clear risk responsibility** (commercial and legal risk responsibility) with the line management and process ownership for the risk management function. Small to medium size organisations who cannot afford a full time risk manager may consider outsourcing the ownership for the risk management process, not the actual risk responsibility, however.

6. Define a maturity concept for the implementation and further development of risk management and its key instruments to be used: Start small and simple, but define a **clear road map** in which direction the organisation's risk management should go in the mid-term future, for example, the next five years.

7. Combine **qualitative and quantitative risk evaluation** methods and avoid too complex quantification exercises in the beginning. Try to generate an enterprise-wide perspective on all risk categories with integration of operational risk scenarios into the market and credit risk analysis.

8. Be aware that enterprise-wide risk management is not just a onetime exercise, but a **continuous improvement process** which will also require change management, adjustments to the IT-landscape, data-warehousing etc. This may cost money on one side, but also assure that risk management moves from a cost centre perspective to a value adding management instrument.

9. **Include outsourced processes** into your risk analysis. Whether the process is an in-house process or an outsourced process (e.g. support processes in HR, IT, Finance etc.) is of less importance as the risk impact of failures in processes, systems or errors of employees is finally remaining on your organisation's balance sheet. Therefore, a systematic risk management approach will also include outsourcing providers into the risk analysis and the risk mitigation action plan.

10. For the IT-support in the risk management process one should **test risk management concepts first on standard office tools** [for example, Excel]. Once the concept has been proven in a pilot case, it is better to move on for the daily operations to an efficient IT-solution with a database, simple workflow support, complete and auditable data history and a granular role and user rights concept. The solution should also allow growing along your maturity concept for the risk management since it may take five years for a full rollout of your concept. Mid to smaller size

organisations may also consider an outsourced IT-solution combined with content related support on risk management.

REFERENCES

CapCo (2003): Understanding and Mitigating Operational Risk in Hedge Fund Investments, White Paper.

Bank for International Settlements (2001): Operational Risk, Consultative Document, Basel Committee on Banking Supervision.

Bank for International Settlements (2009): Results from the 2008 Loss Data Collection Exercise for Operational Risk, Basel Committee on Banking Supervision.

Brammertz, Willi (2009): Unified financial analysis, Wiley Finance.

ORX Operational Risk Reporting Standards (2011), www.orx.org.

van der Aalst, W., Desel, J., Oberweis, A. (2000): Business Process Management: Models, Techniques, and Empirical Studies, Springer Verlag.