Alternative Investment Analyst Review™

What a CAIA Member Should Know

Operational Risk Management in Practice: Implementation, Success Factors and Pitfalls

Claus Huber, CEFA, CFA, FRM, and Daniel Imfeld

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 these institutions to have state-of-the-art operational risk management systems in place. In this article, we focus on operational risk management for mid-sized asset management companies that are not part of a large international banking organization and hence do not have fully developed staff departments for operational risk, compliance, or internal control. Many of these functions in mid to small size asset management organizations will be part-time activities of several people. With regard to operational risk, these mid-size asset managers face many specific challenges, including:

- They have large assets under management, but a small number of employees. The financial assets are comparable to large industrial corporations with several thousand employees.
- Due to their small size, they cannot segregate various duties.
- Increasing cost of compliance and regulatory burden reduces available resources.
- They need to provide a creative business environment for portfolio managers and structured products developers.
- Young organizations typically lack 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 organization can develop systematically an integrated perspective on its main risks and can set priorities on how to mitigate and control these risks.

A pragmatic instrument supporting such an integrated risk perspective is a loss-severity (impact) / loss-likelihood (frequency) matrix or risk map as illustrated in Exhibit 1. It provides an overview for all risks analyzed on the

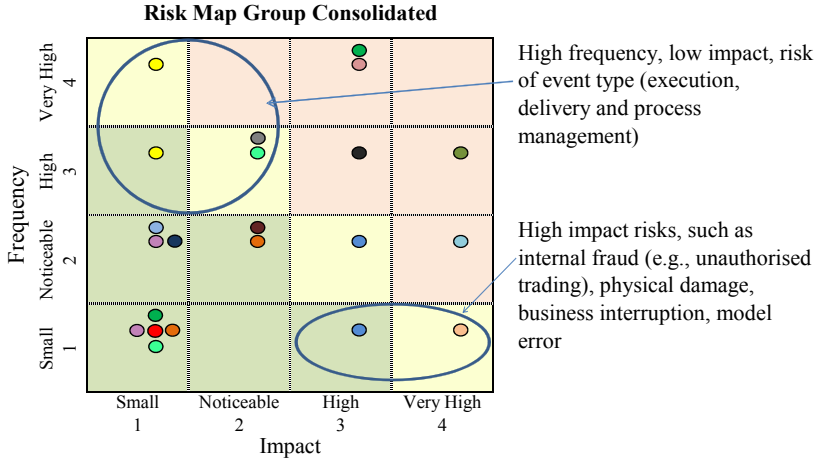


Exhibit 1 Risk Map
Source: SME Risk Platform: RFM Dr. Imfeld, Acons Governance & Audit AG, Avanon / Thomson Reuters

company level; each bullet representing the expert assessment result of an identified risk scenario. 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 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. However, 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 problem complying with regulatory requirements. However, in companies that only look for the regulatory minimum and have little interest in how to implement operational risk management, 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.
- An illustration of key operational risks based on a generic process model for asset management activities.
- An outline of the key steps in a systematic operational risk management process illustrated for one specific risk scenario. We show: (1) how structured risk identification and documentation works, (2) how mitigation measures and controls for the risk can be implemented and tracked systematically, and (3) how continuous reporting allows follow-ups on the status of risks and action plans.
- 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.

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 organization, 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 statement 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 (strategic) risks. The policy describes the main principles for how the organization 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, organization, methods and instruments, IT-solution, and risk communication. Over time (and it will take years rather than months) the integrated risk management framework will encourage responsible functions in the organization 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 organization. Which risks may endanger the success of the company and the

achievement of the company goals? Only based on an integrated risk perspective, as illustrated in the risk map in Exhibit 1, the board and the management team are able to prioritize 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 based on an enterprise-wide risk perspective will help to:

- Prioritize and focus on key risks and risk combinations that may endanger the company's goals and mitigate them with efficient, company-wide mitigation measures and controls.
- Save costs by avoiding unnecessary hedging, insurance, security measures, or by reducing the number of unnecessary controls for risks with only negligible 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 Basel II or ORX documents).

In this context it is important 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 are 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.

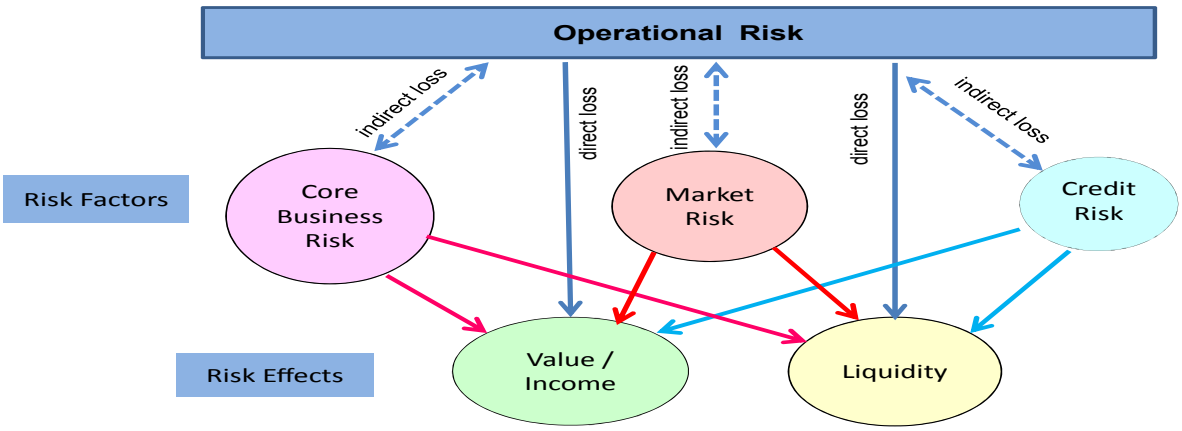


Exhibit 2 What is Operational Risk?
Source: RFM Dr. Imfeld and W. Brammertz

Operational 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 baseline scenario for market data
- Unauthorized trading and 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

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

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

1. A clear risk concept and a categorization that covers all operational risks.
2. An end-to-end basic process model for the key processes in the organization.

3.1. Risk concept and categorization

The first important structural element in the operational risk management framework is a clear risk concept with, ideally, an enterprise-wide categorization of risks. To this end, a company-specific risk framework is beneficial. The event-type risk categorization concept based on Basel II or the ORX can provide helpful guidance as a template and first step towards a company-specific risk categorization. In Exhibit 3, the basic idea for risk categorization, based on risk events, is illustrated. Each event can have one or more causes and several impact types. Causes are often categorized as: people, process, systems, and external causes.

How could this risk categorization be applied in practice? Consider the example of unauthorized trading. History has seen several high-profile breaches of investment guidelines and limits. One of the most prominent examples in the recent past was the unauthorized trading by Jerome Kerviel, which led to a loss of EUR 4.9 billion by his employer, Société Generale, in 2008. In September 2011, UBS lost USD 2.3 billion because of unauthorized trading of one of its employees, Kweku Adoboli. This risk event 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 "unauthorized 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 categorizations of Basel II or ORX can provide guidance for defining company-specific operational risk categories. The categorization helps to avoid confusion about risk causes, risk events, and the impact of a risk. It also allows one 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. Exhibit 4 gives an overview of operational risk loss events by the Basel II main risk event type categories. It shows that process failures cause the largest amount of operational losses for asset managers (53%), followed by clients, products and business practices (31%) and internal fraud (11%). The latter includes unauthorized trading.

3.2. 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 organization and an understanding of critical process interfaces is a good starting point for systematic and successful risk identification.

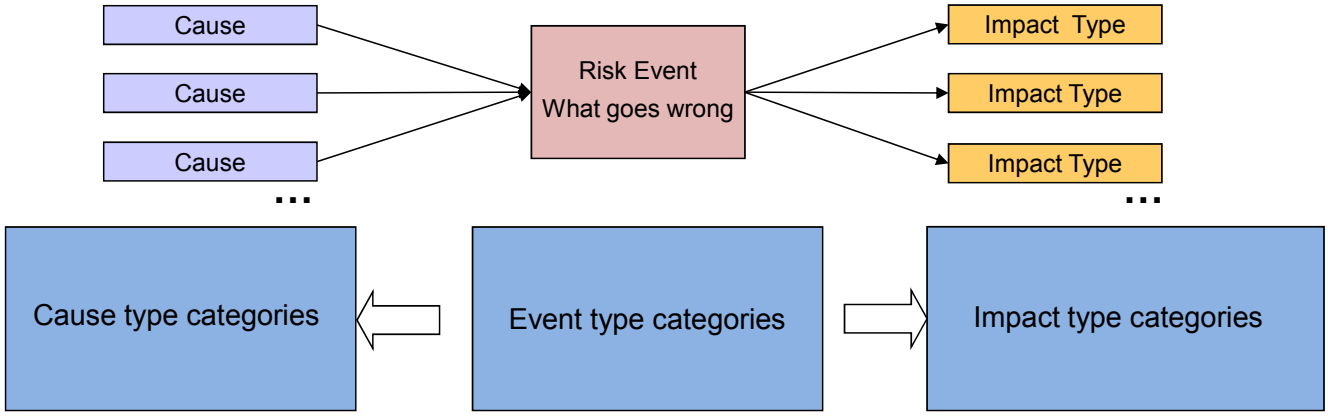


Exhibit 3 Event / Cause / Impact risk categorization

Exhibit 4 Distribution of annualized loss amounts by event type for asset management units of banks

	Internal fraud	External fraud	Employment practices and workplace safety	Clients, products and business practices	Damage to physical assets	Business disruption and system failures	Execution, delivery and process management	All
in EUR millions	27	2	6	75	1	4	128	243
in %	11%	1%	3%	31%	0%	1%	53%	100%

All identified risks are allocated to a specific process and an organizational unit in order to assure clear ownership in the line management for specific risks. Large organizations often maintain fully developed process models in a specialized process management department. For smaller- or mid-size organizations, 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 that can help to systematically identify risks.

In Exhibits 5a, b, and c 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. Consider, for example, the event "unauthorized trading and style breach;" i.e., the breach of investment guidelines. The risk will mostly occur in the process related to asset and portfolio management, which belongs to the core business processes in Exhibit 5b.

Based on the two conceptual elements, risk categorization and process model, we make sure to cover the relevant universe of risks in the organization. A matrix similar to Exhibit 6 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.

4. Systematic Operational Risk Process

Based on the example, fraudulent breach of investment guidelines and investment limits, from our risk list in Exhibit 5b, we illustrate the systematic risk management process from risk identification and/or risk reassessment to mitigation, controlling, reporting, and to defining a risk strategy in line with the risk policy. Exhibit 7 provides structured documentation for identified risks, mitigation measures, and controls. The illustrations are based on anonymized examples recorded on an IT-Operational Risk platform for SME clients. 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 the status level of the control system at any management level.

Assume that 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.

Exhibit 5a Operational Risk Events by Management Processes

Management Processes				
Process Name 1st Level	Process Name 2nd Level	Operational risk events risk scenarios: what can go wrong	Impact	Cause
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 centralized database or only fragmented data about operational risk available	Recurring operational risk incidents causing losses and binding resources	Inadequate systems to deal with operational risk
	Market Risk	Error in risk model: for example, wrong duration for a high yield bond	Portfolio overhedged, unwanted P/L	People, processes, systems
		System breakdown	Portfolio manager is left without reliable sensitivities ("flying blind")	System, datafeeds
	Credit / Counterparty Risk	Non-consideration of credit risk from complex, badly documented structured product	Wrong estimate of credit risk exposure, higher credit risk than realized	Bad maintenance of Excel based documentation, data not in standard system
		Wrong calculation of credit risk exposure, exceeding credit risk limits on consolidated group basis	Wrong estimate of credit risk exposure, higher credit risk than realized	Old, not up-to-date, counterparty data for group structures of counterparties
		Access to liquidity impeded, forced liquidation	Margin requirements increased due to market volatility, credit lines frozen, liquidity management not prepared	Prime broker going bankrupt, market volatility
	Liquidity Risk	Asset liquidity: for example, low market liquidity not adequately reflected in risk tools, thereby underestimating value at risk	Risk figures underestimating actual risk	Inadequate systems to reflect liquidity risk, people
		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 asynchronies

Source: RFM Dr. Imfeld, Rodex Risk Advisers

Exhibit 5b Operational Risk Events by Core Business Processes

Core Business Processes				
Process Name 1st Level	Process Name 2nd Level	Operational risk events risk scenarios: what can go wrong	Impact	Cause
Product Development	Product Development	Wrong documentation of risk exposure in the product	Liability law suit for faulty consulting of clients	Process, people
Sales	Sales	Inappropriate sale and consulting related to complex products for non-institutional clients	Liability law suit for faulty consulting of clients	Process, people: lack of training, badly designed incentive system for sales force
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, and technology
		Unauthorized trading and style breaches, breach of investment guidelines	Market risk, sanctions (fine) as a result of non-compliance, damaged reputation	People, insufficient controls, and processes

Exhibit 5c Operational Risk Events by Support Processes

Support Processes				
Process Name 1st Level	Process Name 2nd Level	Operational risk events risk scenarios: what can go wrong	Impact	Cause
Treasury	Liquidity Management, Hedging etc.	Unwanted market risk exposure inadequately 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 performance restatements can lead to investors losing confidence in processes	People, processes
		Data processing error. An investor in a PE fund of funds, NAV and unfunded commitments need to be taken from capital account statements, put into the PE FoF's systems, then transferred 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 business	Delay in data delivery, inadequate systems
	Management Reporting	Delayed and incomplete reporting	Wrong assumptions for business decisions, market risk	Inappropriate systems
	Reporting to Investors	Fraudulent 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	Fines imposed by regulator	People, processes, systems
HR	Recruiting	Inadequate resources for fund strategies	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 proprietary software development as a base for new products	Delay of market launch of new product	Process: unrealistic planning People: lack of resources

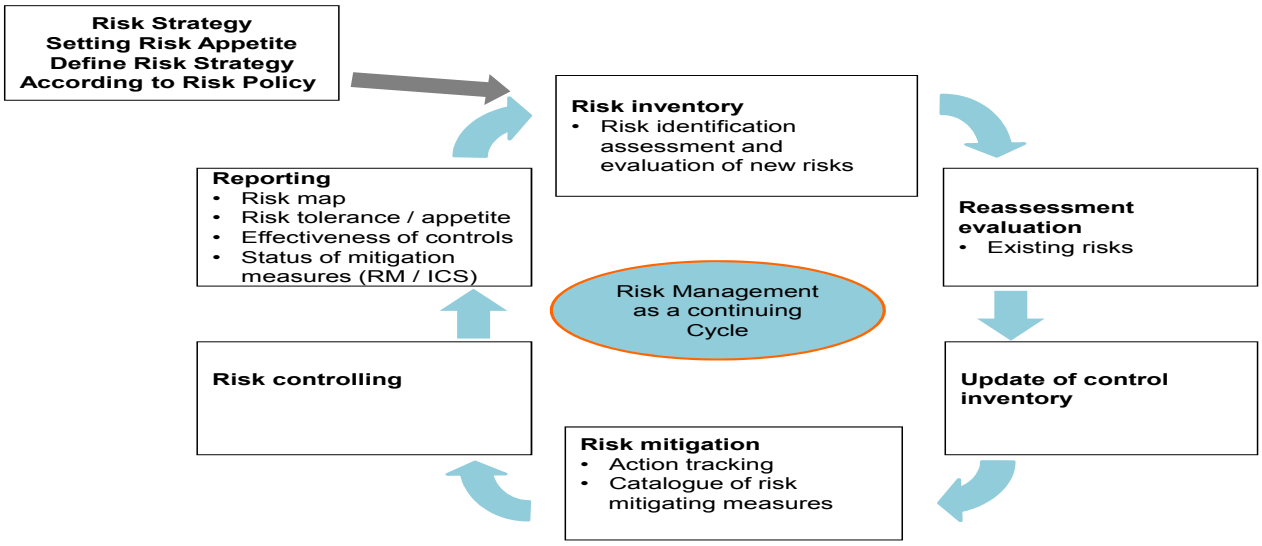
Source: RFM Dr. Imfeld, Rodex Risk Advisers

Exhibit 6 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							
Management processes							
Strategy process and business planning				x			
Risk Management, Internal Control	x			x		x	x
Core Business Processes							
Product Development							
Sales		x			x		
Asset Management process							
Support Processes							
Treasury						x	x
Finance / Back office			x				
HR			x				
Procurement						x	x
IT							x

Source: RFM Dr. Imfeld, Rodex Risk Advisers

Exhibit 7 Iterative risk management process



Source: RFM Dr. Imfeld

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 (Exhibit 8).

In our example, the risk scenario referred to as "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" (see Exhibit 8). A by-product of the risk identification step is that the people in the organization 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 and addressed. In Exhibit 8 we illustrate a minimum of structured information that is collected for each risk scenario in the risk inventory database.

Additional important points in this table are that the risk is made visible to people in the organization, 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 Exhibit 9). 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.

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 Exhibit 9). A key control for our example could be to introduce a four-eyes principle on transactions exceeding EUR 1 million (see Step 2: Risk Mitigation and Control System).

A mid-size 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 the assessment to the top 10 risks only. If 30-50 risks are reassessed systematically in a certain frequency (e.g., annually), chances are high for identifying 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 a watch list.

Exhibit 8 Structured risk assessment, information stored in the risk inventory

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 organization
Impact Types	Accounting, profit and loss and balance sheet Financial impact on assets Reputation Cash flow, liquidity
Organizational Unit	/ 99.9 financial institution / company X AM
Process	4. asset management / 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

Source: SME Risk Platform by RFM Dr. Imfeld, Acons Governance and Audit AG, Avanon / Thomsom Reuters

Exhibit 9 Frequency / severity assessment

Risk Scenario Assessment in terms of impact and frequency				
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	Xcritical	o catastrophic

Source: SME Risk Platform by RFM Dr. Imfeld, Acons Governance and Audit AG, Avanon / Thomsom Reuters

B. Other Risk Identification Instruments:

Risk scenario identification is usually the first and simplest method to implement for mid-size 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 systematically collecting information on past actual loss events. It is useful to learn from one's own or other organizations' historical risks that materialized in an actual loss or resulted in a near miss. These methods are widely used in airlines or hospitals, and to some degree 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, and 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, and law suits with contingent liabilities where actual reserves are marked on the balance sheet.

Industry-specific loss statistics and loss databases for operational risks are available from a variety of sources including the Bank for International Settlements, from whose reports the data in Exhibit 4 was 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 turbulent periods 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 organizations 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 analyzing 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 organization'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 Exhibits 10 and 11). 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 finalized,
- "Active:" the documentation is approved and actions can be implemented and risks can be reported, and
- "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 Exhibit 10).

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-eyes 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 Exhibit 11 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

Exhibit 10 Risk Mitigation

Mitigation measure	
Reference Id	ORAP-20110704-00001
Type	Action Plan
Type of mitigation measure	Risk Management / Strategy
Short Description / Name	Personnel policy and four-eyes 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 Organizational 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

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

Exhibit 11 Internal control

Internal Control	
Reference Id	ORAP-20110704-00003
Type	Internal Control System, Financial Reporting Control/Operations Control
Short Description / Name	Four-eyes principle on PM transaction with size exceeding EUR 1 ml.
Description of Control	Double signature required for transactions in PM exceeding EUR 1 ml. 2nd signature required from employees of same or higher hierarchical level.
Responsible Organizational 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	--

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

optimizations. For example, once per month the responsible person receives an email listing of all "Temp" items.

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 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 keep an up to date perspective and allow timely reporting on the status of risks, mitigation measures, and controls. The dashboard function shown in Exhibit 12 gives an idea of how the risk and control function can make use of the structured information on risk scenarios, 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 upper part of the dashboard overview (see Exhibits 12a, b, c, d) shows all identified operational risks for the asset manager. For illustration purposes, we show only four different risks. A short description of each risk is displayed, together with the risk owner and the status (temporary, valid and archived). The risk map (Exhibit 12a) 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 (i.e., noticeable frequency with very high impact). In the lower part of the dashboard an overview (see Exhibits 12d and c) on the status of mitigation measures and the implementation of controls is given.

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 dashboard is in the overall management information system and business planning.

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

The basic steps of the risk management process are performed for our example risk "fraudulent breach of guideline/limits." The risk is identified and 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. For example, relatively simple methods can be introduced to allow grouping of risks by categories to look for worst case risk scenarios, consolidating risks across business units, and evaluating dependencies, correlation, or diversification potential between risks. This is 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 organization.

The risk manager is able to produce risk reports according to the need of any type of management level based on the structured risk information gathered and the integrated perspective on all relevant risks, mitigation measures, and implemented controls. 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 following questions:

- Which risks need further mitigation and a prioritized 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 it to save costs in insurance, hedging, and unnecessary security measures, or to save time by giving up unnecessary control activities.
- Which risks diversify within the organization? Often risks seem important from one department's point of view, but for the organization as a whole the risk is diversified and acceptable.

Exhibit 12 Dashboard Overiew

Exhibit 12a Risk Map

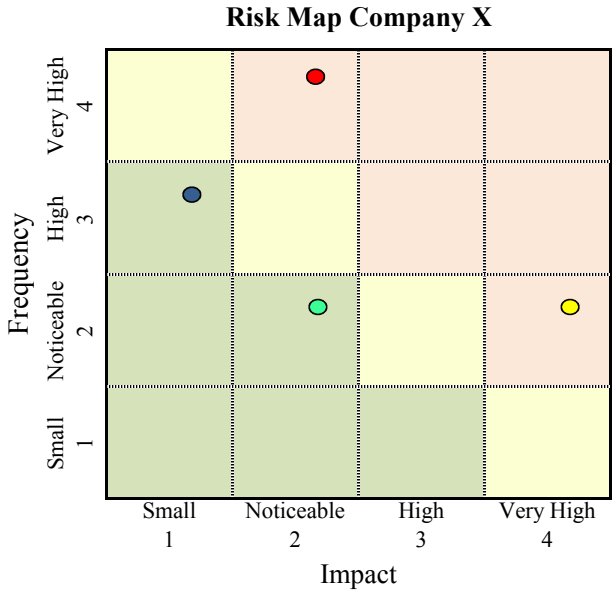


Exhibit 12b Risk by Process

All Risks by Process		
Short Description / Name	**Risk Owner**	**Status**
Wrong data due to manual interface based on Excel spreadsheets	Mister M	VAL:Valid
Wrong data due to missing data control within fund management outsourcing partners	Asset Manager	VAL:Valid
Errors in counterparty analysis for creadit derivative transactions	--	VAL:Valid
Fraudulant breach or exceeding of investment guidelines and investment limits	Head Portfolio Management	VAL:Valid

Exhibit 12c Overview Control Tasks

Overview Control Tasks		
Name	Contact Person Tool	Status
Sign-off Compliance Statement Results: 1 - 1/1	User 2, Test-Demo (Test-Demo)	COMP: Completed

Exhibit 12d Overview Action Plans

Overview Action Plans			
Short Description / Name	Target Date	Responsible for Measure	Status
Inroduce process for systematic data review and comparison with outsourcing data provider	2011.04.01	Asset Manager	TEMP: Temporary
Access to outsourcers control system and audit report on operational risk	2011.06.01	Compliance Officer	TEMP: Temporary
Inroduce strict four-eyes principle for transactions with size>2 Mio. USD	2011.12.08	Head of Personnel	TEMP: Temporary

- 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 if 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 materialize?

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 center 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 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, organization, 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 of how the organization manages its risks and briefly 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 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. 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 a 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 organizations who cannot afford a full time risk manager may consider outsourcing the ownership for the risk management process, but not the actual risk responsibility.
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 organization'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 one-time exercise, but a continuous improvement process that will also require change management, adjustments to the IT-landscape, data-warehousing, etc. This may cost money on one side, but also assures that risk management moves from a cost center 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) is of less importance than whether the risk impact of employee errors or failures in processes, or systems falls upon the organization'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 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 your maturity concept for the risk management, since it may take five years for a full rollout of your concept. Mid to small size organizations may also consider an outsourced IT-solution combined with content related support on risk management.

References

CapCo. "Understanding and Mitigating Operational Risk in Hedge Fund Investments." White Paper, 2003.

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

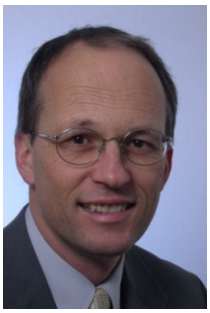
Bank for International Settlements. Results from the 2008 Loss Data Collection Exercise for Operational Risk, Basel Committee on Banking Supervision. 2009.

Brammertz, W. "Unified Financial Analysis." Wiley Finance, 2009.

ORX Operational Risk Reporting Standards. www.orx.org. 2001.

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

Author Bios



Since 2002 **Dr. Daniel Imfeld** has served as an independent adviser and project manager in enterprise-wide and operational risk and control management. He is consultant to financial services companies (insurance, banks) and non-financial corporate clients (Energy, Telecom, Technology, Hospitals, Pharma, Administrations). Daniel Imfeld specializes in risk strategy and corporate finance, implementing enterprise-wide risk management from strategy to IT-supported processes, risk management organization and process, risk and financial modelling, DFA, Solvency II, developing innovative risk solutions. In the German-speaking markets Dr. Imfeld is leading the consulting efforts for insurance and industrial clients of the Avanon AG/ COMIT AG partnership. Dr. Imfeld has managed several consulting and implementation projects related to Avanon and IRIS/FRSGlobal software solutions for enterprise-wide and operational risk management. (contact: daniel.imfeld@rfm-imfeld.ch, 0041 (0)41 761 18 92)

Since June 2010 Dr. **Claus Huber**, CEFA, CFA, FRM, has been running Rodex Risk Advisers, a risk management consultancy. A few of the topics covered are tail risk insurance, inflation and deflation protection, and market and operational risk. The Rodex Purchasing Power Protection Indices, an investment solution to protect against inflation and deflation, won the Swiss Derivative Award 2012. In a previous role as Head of Alternative Investment Risk Management at Swiss Re Zurich from 2008 to 2010, he built and integrated the risk management function for Hedge Funds, Private Equity, and Real Estate into the Swiss Re risk management framework. There he dealt with, amongst others, the development of stress tests and value-at-risk-models, concepts of valuation and hedging illiquid assets, the interest rate sensitivity of real estate assets, building a managed account for a fixed income arbitrage hedge fund, and examining the risk/return profile of hedge funds. In a prior role as Chief Risk Officer at Credaris Portfolio Management, London, from 2004 – 2007, Claus developed and implemented the risk management framework for a credit hedge fund. From 2000 to 2004 he worked as a Credit Strategist and Hedge Fund Analyst at Deutsche Bank in Frankfurt/Main. During a stint as a research associate from 1996 to 1999 at the University of Bremen / Germany he wrote a dissertation about forecasting turning points in financial markets with econometric models. At Bankgesellschaft Berlin he traded government bonds from 1994 to 1996. Claus has published numerous papers on various topics in Finance.