18

Operational Risk Management for Hedge Funds

CLAUS HUBER
Founder and Managing Director, Rodex Risk Advisers LLC, Altendorf / Switzerland

DANIEL IMFELD
Owner and Founder of RFM Dr. Imfeld, Risk and Finance Management,
Partner of Ariadne Business Analytics AG in Switzerland

Introduction

According to the often-cited CapCo (2003) study about hedge fund failures, operational risk was the driving force of 50 percent of those failures. Operational risk management (ORM) is increasingly important not only for hedge funds but also for other asset managers such as private equity companies, family offices, and independent asset managers. Pressure from investors and regulators as well as increasing market competition require state-of-the-art ORM from these institutions. This chapter focuses on ORM for midsize hedge fund companies, which are not part of a large international organization and lack fully developed staff departments for operational risk, compliance, or internal control. Many of these functions in mid- to smaller-sized hedge fund organizations are part-time activities of several employees. Regarding operational risk, these midsize hedge funds face many specific challenges:

- Having large assets under management (AUM), but few employees
- Experiencing difficulty segregating duties
- Facing increasing regulatory focus and burden
- Creating a creative business environment for portfolio managers and product structurers
- Being younger organizations with no tradition of risk and control management or structured processes

This chapter takes a practitioner's view of how to implement an operational risk framework as part of an enterprise-wide risk and control system in a "hands-on" approach. It outlines how a midsize hedge fund organization can systematically develop an integrated perspective on its main risks and set priorities on how to mitigate and control these risks.

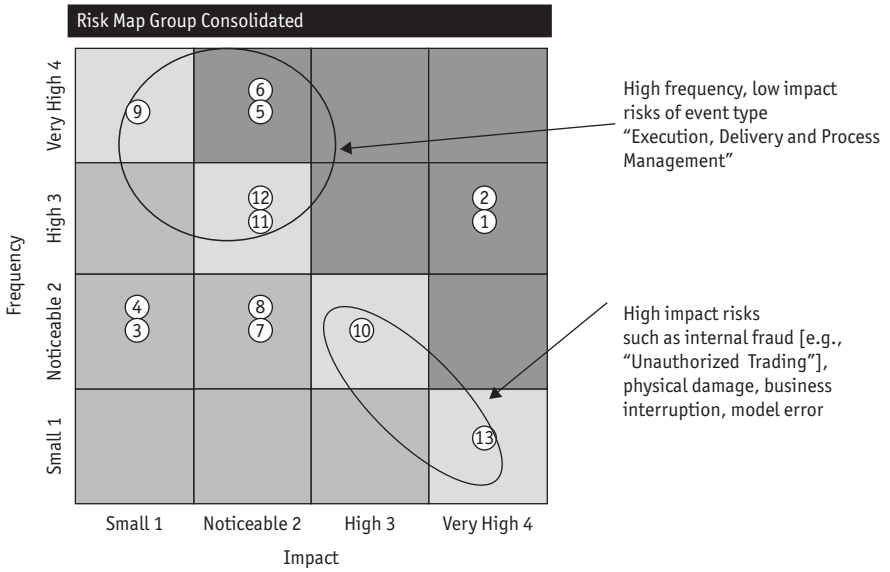

Figure 18.1 **A Risk Map.** This figure shows a loss-severity (impact) / loss-likelihood (frequency) matrix or risk map. Large risks that occur at a high frequency are shown in the upper-right zone, smaller and less frequently occurring risks in the lower-left zone. *Source*: RFM Dr. Imfeld.

A pragmatic instrument supporting such an integrated risk perspective is a loss severity (impact) / loss likelihood (frequency) matrix or risk map, as Figure 18.1 illustrates. The risk map provides an overview for all risks analyzed on the company level, each bullet representing the expert assessment result of an identified risk scenario. Large risks are shown in the upper-right zone with high impact and high frequency, smaller risks accordingly in the lower-left zone. The upper-left corner shows high-frequency but low-impact risks often related to a process or quality issues, whereas the lower-right corner plots rare but catastrophic risk scenarios.

Many companies still view ORM only as a regulatory burden and a cost factor. Yet practical experience shows that companies profit from ORM 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 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, ORM 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.

The remainder of the chapter has the following organization. The first section provides an overview of the academic literature on operational risk, followed by a section on the terms used and how risk management needs to be designed to add value. Next, an illustration of key operational risks is provided based on a generic process model for asset management and hedge fund activities. The chapter then provides an outline of

the key steps in a systematic ORM process, illustrated for one specific risk scenario. The chapter shows how a structured risk identification and documentation works, how mitigation measures and controls for the risk can be implemented and tracked systematically, and how continuous reporting allows follow-ups on the status of risks and action plans. Further discussion involves dealing with the critical issues of operational risk in outsourced processes and the automation of control confirmation, risk controlling, and reporting based on standard information technology (IT) tools. The final section highlights typical success factors and pitfalls in the implementation from the concept phase to the introduction of an IT-supported risk management process.

Operational Risk in the Academic Literature

This section provides a selective overview of academic studies on operational risk of hedge funds. It provides a few key takeaways for the practitioner rather than a complete survey of the literature. Academic papers on operational risk of hedge funds use data from three sources: (1) performance analysis, (2) publicly available information (e.g., Form ADV), and (3) private information (e.g., due diligence reports). One example from performance analysis is by Bollen and Pool (2009), who investigate the effect that the number of small gains in hedge fund returns far exceeds the number of small losses. This relation can occur because some managers may be rounding up returns to achieve specific return targets.

Studies on publicly available information often draw on the data provided by Form ADV of publicly available hedge fund filings to the Securities and Exchange Commission (SEC), available at www.adviserinfo.sec.gov. Each Form ADV contains 12 items. Brown, Goetzmann, Liang, and Schwarz (2009) use item 11 to identify any potential problems of the funds (e.g., felonies, investment-related misdemeanors, civil lawsuits, and any regulatory issues). Thus, a hedge fund with an entry in item 11 is categorized as a problem fund that has high operational risk. By analogy, nonproblem funds are categorized as low operational risk. Brown et al. find statistically significant differences in variables reflecting potential conflicts of interest between problem funds and nonproblem funds. For example, 85 percent of problem funds allow their personnel to buy and sell securities owned by the fund, while only 16 percent of the nonproblem funds do. This finding suggests that the potential for conflicts of interest can lead to operational risk events. Generally, Brown et al. contend that funds with more conflict-of-interest issues, concentrated ownership, and lower leverage ratios tend to have higher operational risk. Also based on Form ADV, Dimmock and Gerken (2012) identify, for example, past regulatory and legal violations of the asset manager as predictors of fraud. Another useful indicator is that monitoring, such as trading through an affililated broker-dealer rather than an external firm, can remove one form of external oversight and provide a mechanism for fraud. The most important takeaway for the practitioner is the fact that Form ADV can hold important information for the assessment of a hedge fund's operational risk.

Brown, Goetzmann, Liang, and Schwarz (2012) provide an example of research coming from the area of private information. The authors analyze 444 hedge fund due diligence reports for indications of operational risk. They find that 41 percent of hedge funds have had previous regulatory issues or lawsuits. This result is about twice the percentage based on Form ADV filings and shows that self-representation even under

regulatory pressure provides an overly positive picture. In 16 percent of the sample, the fund's explanations of the signature processes (e.g., how many signatures are needed to transfer money) did not match the administrator's version. Misrepresentation of a manager's background took place in 21 percent of the funds in the sample. A total of 18 percent of funds' asset information either could not be verified independently or disagreed with evidence from an alternative source. Brown et al. report performance disagreements or verification problems for 14 percent of the due diligence reports. Cassar and Gerakos (2010) find evidence that using more reputable outside service providers (e.g., for auditing services) reduces the likelihood of fraud. The same applies for prime brokers providing leverage, as providing leverage introduces another stakeholder in the fund's performance and operations that is likely to demand that funds implement strong internal controls as precondition for providing credit. Hence, a fund using leverage positively affects internal controls.

In summary, operational risk can be measured by collecting publicly available information, such as Form ADV, or by private due diligence reports. Strong processes within the firm and internal controls are indicators of low operational risk. Hence, the remainder of this chapter discusses how to strengthen processes and implement effective controls.

Adding 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 ORM and internal controls as an integral part of the enterprise-wide risk and control management system. Because risk management activities involve many functions in the organization, such as asset liability management, operational risk, internal control, internal audit, security and business continuity management, and compliance, setting up an integrated risk and control framework based on one risk policy is important.

To start, a risk policy should be defined as a short (one to three 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 includes market, credit, and core business or strategic risks. The policy describes the main principles for how the organization manages its risks and 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, the integrated risk management framework encourages responsible functions in the organization to develop a common enterprise-wide understanding of risks as a basis for better business decisions.

A starting point of each risk management activity is identifying potential risks and assessing their relative importance for the organization. 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 18.1, can the board and management prioritize key risks and 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 can help in the following ways:

- Prioritize 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 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
- Ensure adequate but realistic crisis management and business continuity measures that allow business survival in critical periods. Often simple measures can have a dramatic (positive) impact.
- Actively manage and reduce operational risks to avoid surprises and simultaneously add value by consciously allowing investing more risk capital for the core business and wanted market or credit risk
- Ensure compliance with regulations

NATURE OF OPERATIONAL RISK

Operational risk describes possible risk events leading to an actual outcome of a business process that differs from the expected or targeted outcome. These events can be due to inadequate or failed processes, to people and systems, or to external facts or circumstances. In this context, an understanding that operational risks often cause and drive credit, market, and core business or strategic risks is essential to the process. Figure 18.2 highlights operational risk events than can have a direct or indirect impact on a company's value and earnings or the liquidity available.

For example, a direct effect of a physical business interruption can result in a loss of operational assets or loss in revenue. However, the indirect effects via market, credit, or core business risks of such a business interruption can be much higher than direct losses (e.g., due to the inability to buy or sell assets as planned or necessary according to a client agreement or required due to high market volatility). In rare cases such as extreme market or credit risk volatility, market and credit risk could cause unexpected operational risk events because of a breakdown of the standard processes in such a period.

A Process-Based Approach for Operational Risks

This section systematically develops a full picture of the operational risks the organization is facing. The following two conceptual elements ensure coverage of the whole risk universe: (1) a clear risk concept and a categorization that covers all operational risks and (2) an end-to-end basic process model for the key processes in the organization.

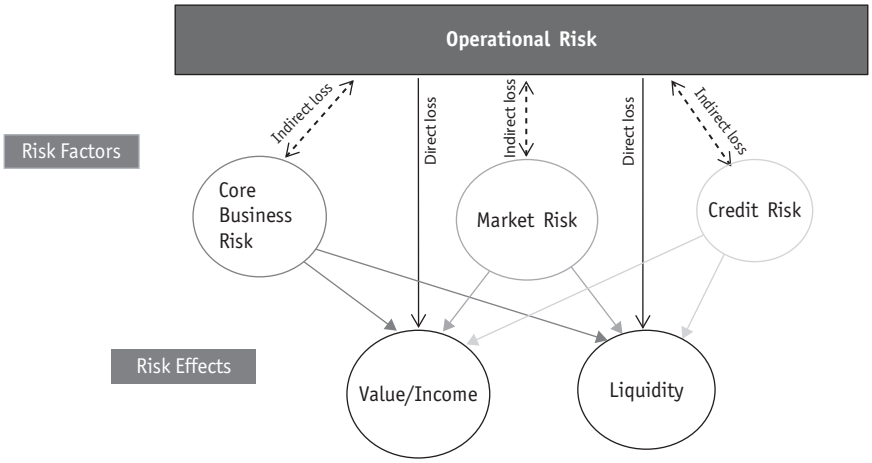

Figure 18.2 **A Flow Diagram of Operational Risk.** This figure shows the dependence between operational risk as driver of potential market, business, or credit risk and illustrates that all risk sources have a value, income, and liquidity impact. *Source*: RFM Dr. Imfeld and W. Brammertz.

RISK CONCEPT AND CATEGORIZATION

The first important structural element in the ORM 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 concept of a risk categorization based on event cause and effect type is based on Basle II (Bank for International Settlements 2001) or the Operational Risk Data eXchange (ORX 2011). Operational risk reporting standards can provide helpful guidance as a template and first step toward a company-specific risk categorization.

Figure 18.3 illustrates the basic idea of risk categorization. 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 types are the often-used categories: people, process, systems, and external causes.

How could this risk categorization be applied in practice? Several high-profile breaches of investment guidelines and limits are available. One prominent example is the unauthorized trading by Jerome Kerviel, which led to a loss of EUR 4.9 billion at his employer, Société Generale, in 2008. In September 2011, UBS lost USD 2.3 billion because of unauthorized trading by Kweku Adoboli, one of its employees. This risk is infrequent, 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 negative headlines in the press.

The official categorizations of Basle II or Operational Risk Data eXchange (ORX) can provide guidance for defining company-specific operational risk categories. The categorization helps (1) to avoid confusion about risk causes, risk events, and the impact

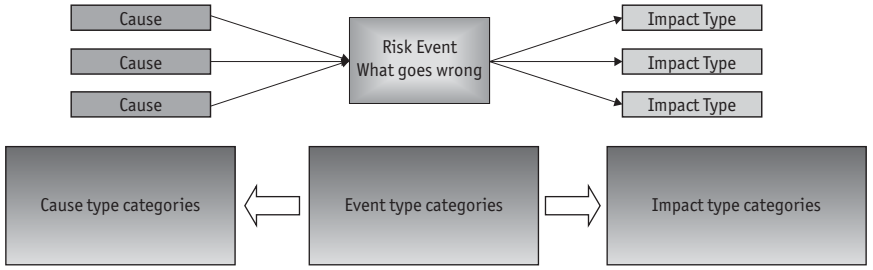

Figure 18.3 **Event/Cause/Impact Risk Categorization.** This figure shows the three dimensions of risk categories used to allow for differentiation between a risk event (what goes wrong), the cause, and the impact of the event. *Source*: RFM Dr. Imfeld.

of a risk and (2) to allow the ability to group similar risks from the same risk event category and to support a more efficient design of mitigation measures for similar risk events or risks with the same cause. Operational risk loss events by the Basle II main risk event type categories as outlined in Bank for International Settlements (2009) are "process failures" (53 percent of operational losses), followed by the category "clients, products, and business practices" (31 percent), and internal fraud (11 percent). The latter includes, for example, unauthorized trading. Less frequent risk loss events are in the event categories "employment practices and work-place safety" (3 percent), "business disruption and system failures" (1 percent), "external fraud" (1 percent), and finally "damage to physical assets" (less than 1 percent).

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 hedge fund organization and an understanding of critical process interfaces are good starting points for systematic and successful risk identification. All risks identified are allocated to a specific process and an organizational unit to ensure clear ownership for specific risks in the line management. Large organizations often maintain fully developed process models in a specialized process management department. Van der Aalst, Desel, and Oberweis (2000) provide an overview of those models. For smaller or midsize organizations, the operational risk and control management does not require a costly process-modeling infrastructure, but a generic process model with a clear end-to-end perspective can help to systematically identify risks.

Tables 18.1 and 18.2 provide an example of a generic process model for a hedge fund company. For illustration purposes, typical risk scenarios for each process describe briefly, for each scenario, the actual risk event, the cause of the event, and possible impacts. For example, for the event "unauthorized trading and style breaches, breach of investment guidelines," the risk mostly occurs in the process "asset management, portfolio management," which belongs to the core business processes in Table 18.1.

Table 18.1 **Operational Risk Events by Management and Core Business Process**

Process Name First Level	*Process Name Second Level*	*Risk Scenarios: What Can Go Wrong*	*Impact*	*Cause*
Strategy process and business planning	Strategy process	Changing the investment style of the fund without the approval of investors (style drift)	Drift to area of noncore expertise, investors redeeming	People, guidelines
Risk management internal control	Market risk	Error in risk model: e.g., wrong duration for a high-yield bond	Portfolio overhedged, unwanted P/L	People, processes, systems
	Credit/counterparty risk	Nonconsideration 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
	Liquidity risk	Asset liquidity: e.g., low market liquidity not adequately reflected in risk tools	Risk figures underestimating actual risk	Inadequate systems to reflect liquidity risk, people
	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
Product development	Product development	Wrong documentation of risk exposure in the product	Liability lawsuit for faulty consulting of clients	Process, people
Sales	Sales	Inappropriate sale and consulting related to complex products for noninstitutional clients	Liability lawsuit for faulty consulting of clients	Process, people: lack of training, badly designed incentive system for salesforce

(*continued*)

Table 18.1 **Continued**

Process Name First Level	*Process Name Second Level*	*Risk Scenarios: What Can Go Wrong*	*Impact*	*Cause*
Asset management process	Strategic asset allocation process	Data error in baseline scenario for market data	Portfolio implementation too far away from benchmark	Manual interface based on Excel sheets, no auditable data versions
	Portfolio management	Backlog of (derivatives) trades	Market risk	System, people, processes, technology
		Unauthorized trading and style breaches, breach of investment guidelines	Market risk, sanctions (fine) as a result of noncompliance, damaged reputation	People, insufficient controls and processes

Note: This table shows an example of a generic process model for an asset management company.

Table 18.2 **Operational Risk Events by Support Processes**

Process Name First Level	*Process Name Second Level*	*Risk Scenarios: What Can Go Wrong*	*Impact*	*Cause*
Treasury	Liquidity management, hedging, etc.	Unwanted market risk exposure (e.g., wrong FX exposures due to complex spreadsheets rather than robust risk tools)	Unintentional P/L impact, unexpected margin calls and cash impact	System, people, processes
Finance / back office	Accounting, fund administration and documentation (transaction capture, P&L/NAV)	Wrong booking of subscriptions/redemptions (e.g., subscriptions erroneously added to NAV when calculating performance)	Leading to wrong NAV and over-/ underestimating the performance; material performance restatements; investors losing confidence	People, processes
		Data processing	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, system

(*continued*)

Table 18.2 **Continued**

Process Name First Level	*Process Name Second Level*	*Risk Scenarios: What Can Go Wrong*	*Impact*	*Cause*
	HR salary	Wrong data access rights to salary system attributed to employees	Sanction, lawsuit due to noncompliance with privacy laws and privacy policy	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

Note: This table shows a process model similar to that in Table 18.1, but now sorted by support processes.

The Systematic Operational Risk Process

Based on the example "fraudulent breach of investment guidelines and investment limits" from the risk list in the previous section, this section illustrates the systematic risk management process in four steps: (1) risk identification and risk reassessment, (2) risk mitigation, (3) risk controlling/reporting, and (4) defining a risk strategy in line with the risk policy. The illustrations in Tables 18.3, 18.4, and 18.5, show 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 examples are taken from the authors' OpRisk platform that runs on a "Software as a Service" basis specifically designed for smaller and medium-sized companies in the area of finance. It supports risk assessment, control and mitigation measure workflow support, and risk and control reporting. The sample reports show how to systematically gather structured information on risks, keep up with risk mitigation measures, and ensure that necessary controls are known and performed as expected. The structured information allows straightforward risk analysis and aggregation, as well as simple documentation and reporting on risks, action plans, and status level of the control system at any management level required. Assuming a company has defined the risk management framework and outlined it in the risk policy, the ORM cycle starts with the first implementation step, creating the risk inventory by risk identification and risk assessment.

STEP 1: RISK IDENTIFICATION AND 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. In the example, workshop participants identified the risk scenario "fraudulent breach of investment guidelines and investment limits" as part of the process number 4.1, "Asset Management, Portfolio Management." A byproduct of the risk identification step is that the people in the organization are forced to think about what can happen, who or what might cause the risks, and how to mitigate or address the risks. Table 18.3 illustrates a minimum of structured information that is collected for each risk scenario in the risk inventory database.

Another important point in Table 18.3 is that the risk is made visible to people in the organization, thereby raising awareness, naming an owner for the risk, and clearly assigning responsibilities. Quantifying the potential loss in monetary terms requires collecting additional information about loss frequency (e.g., low, noticeable, high, and very high) and loss severity (e.g., small, noticeable, critical, and catastrophic), as Table 18.3 shows in the lower part. The risk evaluations and quantification are based on expert discussions. Typically, good results for risk evaluations are achieved if unit heads and risk or process experts agree on the evaluation of the risk.

A midsize hedge fund may start its risk inventory from the initial risk assessment with three to five risks per process, adding up to 30 to 50 risk scenarios in the database. Not all of those risks are key risks, but experience shows that not being confined to the top 10 risks is advantageous. If 30 to 50 risks are reassessed systematically in a certain frequency, say annually, chances are high that new risk trends will be identified. Hence,

Table 18.3 **Structured Risk Assessment, Information Stored in the Risk Inventory**

Risk Scenario	
Reference Id	RA-2011-0704
Short description/name	Fraudulent exceeding of investment guidelines and investment limits
Description including 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 Type	1. Accounting, Profit and Loss & Balance Sheet 2. Financial impact on assets 3. Reputation, 4. Cash Flow, Liquidity
Organizational unit	/ 99.9 Financial Institution/Hedge Fund X AM
Process	4. Asset Management./4.1 Portfolio Management
Risk owner	Head Portfolio Management
Contact person tool	Test User
Attachments	0
Status	TMP: temporary
Entry created at	2016.07.04
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	

Note: This table shows an example how structured information for each risk scenario can be collected in the risk inventory database.

Source: RFM Dr. Imfeld, Risk Platform on Different IT-Solutions. Implemented as Software as a Service Solution. (Solution Providers: Thomson Reuters and myGRC of Fecton GmbH.)

Table 18.4 **Risk Mitigation**

Mitigation Measure	
Reference Id	AP-2016-0704-1
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 organizational unit	/Financial Inst./Company X AM/
Process allocation	Financial Institution/4. Asset Mgmt./
Implementation target date	2016.12.08
Priority	High
Cost of measure (in USD) optional	10,000.00
Responsible for measure	Head of Personnel
Contact person tool	User 2, Test-Demo (Test-Demo)
Status	TEMP: Temporary
Internet link (http://...)	—
Attachments	0

Note: This table shows how risk-mitigating measures can be structured and systematically tracked. A risk-mitigating measure, in contrast to a control, is usually a one-time measure for which an implementation date and a responsible person are defined.

Source: RFM Dr. Imfeld, Risk Platform on Different IT-Solutions. Implemented as Software as a Service Solution. (Solution Providers: Thomson Reuters and myGRC of Fecton GmbH.)

defining the top 10 list out of 30 to 50 main risks and keeping the other risk scenarios documented in the sense of a watch list is recommended.

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

- Loss data collection on actual loss events. In contrast to potential risk scenarios, identification of operational risks should be based on experience by collecting

Table 18.5 **Control Information**

Internal Control	
Reference Id	AP-2016-0704-3
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 organizational unit	/ Financial Inst./ Company X Hedge Fund/
Risk description	Fraudulent transaction outside of investment guidelines or investment limits.
Relevance of control	Key Control
Process allocation	/ 4. Asset Management/4.1 Portfolio Management
Control frequency	Transactional
Control automation	Manual
IT-Systems	—
Proof of control/evidence	
Control self-assessment	Control to be improved
Responsible for control	Head of Asset Management
Contact person Tool	B-Cooper
Status	TEMP: Temporary
Internet link (http://...) Attachements	—

Note: This table shows an example of how risk control information can be structured and saved.

Source: RFM Dr. Imfeld, Risk Platform on Different IT-Solutions. Implemented as Software as a Service Solution. (Solution Providers: Thomson Reuters and myGRC of Fecton GmbH.)

systematically information on past actual loss events. Learning from an organization's historical risks that materialized in an actual loss or resulted in a "near miss" is useful. Airlines, hospitals, and banks use these methods to some degree. Typical loss event types that are tracked include (1) insured loss events such as liability cases with long-term impact for many years, property losses, theft, and business interruptions with complex multidimensional impact; and (2) uninsured loss events such as customer complaints, internal fraud cases, and major IT breakdowns, data entry errors in

transactions with market or credit risk impact, loss of legal documents, and lawsuits with contingent liabilities where actual reserves are marked on the balance sheet. As discussed previously, industry-specific loss statistics and loss databases for operational risks are available from, for example, the Bank for International Settlements. ORX collects loss events by business segments of large banks. Algorithmics offers a database for financial institutions, covering banks, insurance companies, and hedge funds.

- Key risk indicators of early warning systems 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, leading indicators that may serve as early warning signs for operational risks can be identified. Typical applications include 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 lawsuits with contingent liabilities, employee turnover by department, and 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 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 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

To adequately assess the impact of an identified risk on the organization's business, considering existing controls and mitigating measures that already reduce the likelihood or severity of the risk scenario identified is necessary. A risk-mitigating measure, in contrast to a control, is usually a one-time measure for which an implementation date and a responsible person are defined. How can risk mitigation and controls be integrated in an operational risk framework? This process is illustrated in what follows, with 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, and control) three different statuses and helps to keep track of the implementation steps. Such a workflow support results in improved transparency, efficiency, and data integrity compared to the widespread Excel/Word solutions that typically create problems regarding user access rights, data integrity, and confidentiality. In the simplest workflow, differentiation occurs in the following classifications:

- Temporary: Data entry on risks, risk-mitigating actions, or controls is not yet fully documented.
- Active: The documentation is approved, actions can be implemented, and risks can be reported.

- Completed: Action plans are implemented or risks are being reassessed.

In the example, the risk mitigation measure to be introduced is the establishment of a strict screening process of all individuals who work in portfolio management. As Table 18.4 shows, the head of personnel is responsible for this process. Besides such one-time mitigating measures, the internal control system supports risk mitigation in systematically reducing identified risks to an acceptable level. For the 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 18.5 from the entries in the rows "Status" and "Control Assessment." The risk controller is supposed to follow up on this control and ensure proper implementation. The systematic action and control tracking instrument allows keeping track of pending optimizations. For example, the responsible person receives a monthly 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 the executive team. The risk and control function ensures 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 a current perspective and allow timely reporting on the status of risks, mitigation measures, and controls. Figure 18.4 shows the dashboard function and gives an idea of how the risk and control function uses the structured information on risk scenarios, loss events, key indicators, controls, and mitigation measures.

The first part of the dashboard overview in Figure 18.4 shows all identified operational risks for the hedge fund. For illustration purposes, only four different risks are shown. A short description of the risk is displayed, together with the risk owner and the status (i.e., temporary, valid, and archived). The risk map gives a quick assessment along the two dimensions loss frequency and loss impact. The example risk, "fraudulent breach of investment guidelines and investment limits," shows up in the risk map as the point in the square with noticeable frequency and very high impact. The middle of the dashboard presents an overview on the status of mitigation measures and the implementation of controls. 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 hedge fund transactions are tracked as key risk indicators on the basis of percentage of transactions that show a system error, where up to 1 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 a current picture on the company's overall risk situation 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.

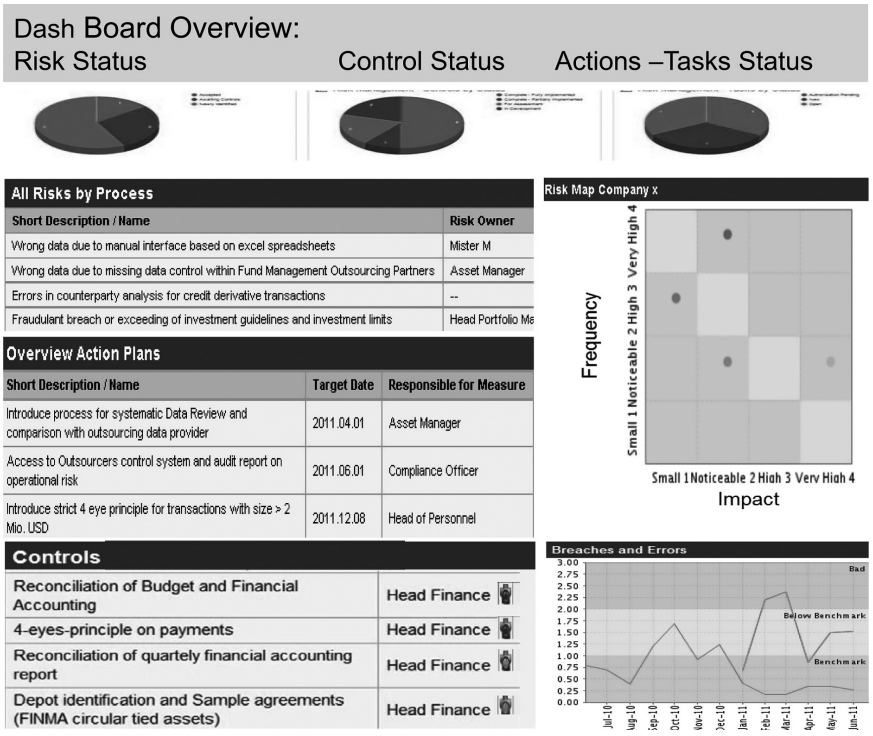

Figure 18.4 **Example of Personal Dashboard Risk and Control Management.** These figures illustrate a group dashboard summarizing information on risk, control, and risk indicator status. *Source*: RFM Dr. Imfeld, Risk Platform on Different IT-Solutions. Implemented as Software as a Service Solution. (Solution Providers: Thomson Reuters and myGRC of Fecton GmbH.)

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

Now the basic steps of the risk management process are performed for the example risk "fraudulent breach of guideline/limits." The risk is identified and an action plan and a control are put in place. But is managing each risk individually efficient? 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 with relatively simple methods and are an important step toward an integrated risk perspective. In an early stage of risk management for midsize hedge funds, engaging in complex quantitative measurement such as aggregated loss distribution estimation based on Monte Carlo simulations or risk capital allocation exercises is unnecessary. But evaluating 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 is worthwhile.

Based on the structured risk information gathered and the integrated perspective on all relevant risks, mitigation measures, and implemented controls, the risk manager can 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 following questions:

- Which risks need further mitigation and a prioritized action plan with approved budget for implementation given that 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 given that the risks are not really threatening company goals? This identification allows saving costs in insurance, hedging, in unnecessary security measures or saving 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 the risk is diversified and acceptable for the organization as a whole.
- Which risks or risk combinations need further analysis and investigation or the development of additional risk evaluation tools, such as an early warning system, detailed scenario modeling, and stress testing or systematic loss tracking?
- Which risks have to be accepted given that 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 materialize?

Working through these steps helps to create value based on a systematic risk management framework and to 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.

Operational Risk in Outsourced Processes

Hedge funds, similar to other midsize financial institutions, rely on outsourced processes in many areas. The industry is moving quickly to a more developed separation of specialized activities in different companies. Hedge funds outsource not only human resources (HR) and information technology (IT) but also investment-controlling back offices, risk and control functions, and regulatory reporting processes.

People tend to think that by outsourcing these processes they can also eliminate the risks in these processes. But an entrepreneurial perspective easily makes clear that this cannot be the case. An outsourced process in an organization that has a poor management of operational risks is no help. Thus, clearly, all outsourced processes belong in the organizations' enterprise-wide risk analysis. From a legal and compliance point of view,

an organization remains responsible to ensure a functioning risk and control management, including all outsourced processes.

Whether the process is an in-house process or an outsourced process (e.g., support processes in HR, IT, and finance) is of less importance as the risk impact of failures in processes, systems or errors of employees remains on the organization's balance sheet. Therefore, a systematic risk management approach should include all outsourcing providers in the risk analysis, control system, and action plans to mitigate risks. Service-level agreements with outsourcing partners should consider this aspect and ensure audit rights to review the risk and control management activities of outsourcing partners. In the evaluation phase of outsourcing, the risk and control management capability of partners needs to be reviewed and considered in the overall offer. If price is the only criterion in the outsourcing evaluation, these aspects are often neglected.

Business contingency plans and business continuity management also need to be evaluated in close cooperation with the outsourcers. Crisis and business continuity management needs to be trained jointly in realistic crisis scenarios; otherwise the crisis training would ignore an important aspect of the organization's processes.

Process Automation

Assessing risks is usually a regular exercise performed by internal experts. Ideally, it is supported by a systematic, continuous risk assessment process in which the frequency of reassessments is defined depending on the type of risks and the frequency of changes in the risk landscape. Reassessments are performed usually on a yearly, semiannual, or at a maximum quarterly basis. Automation of the expert assessment remains difficult. The key aspect in automation is automating recurring controls and checks. Controls are often performed automatically but spread across many IT systems in an organization (e.g., automated controls and checks in a pretrading check, or checks on limits on asset exposures in asset allocation requiring a rebalancing). These automated controls are often complemented in many areas with manual checks and controls. The challenge for management remains to keep the overview and documentation across all process steps, IT systems, and controls, regardless of the medium with which the control or task is performed.

Ideally, the operational risk and control system provides an integrated overview on the status and effectiveness of all manual and automated key controls and mitigation measures by process, department, or whatever is of interest for management. This may require an integration step of information on automated controls with other manually traced controls, as Figure 18.5 outlines.

From different systems on which controls are automatically performed, key information on control performance is automatically saved to a central database. Here, information is allocated and structured along the same process, product, or organizational structure as when it is used for all other manually performed controls. The joint result of reports and evaluation on automated and manual controls is continuously provided in a dashboard or in reports that are actively sent out by email to the relevant management level.

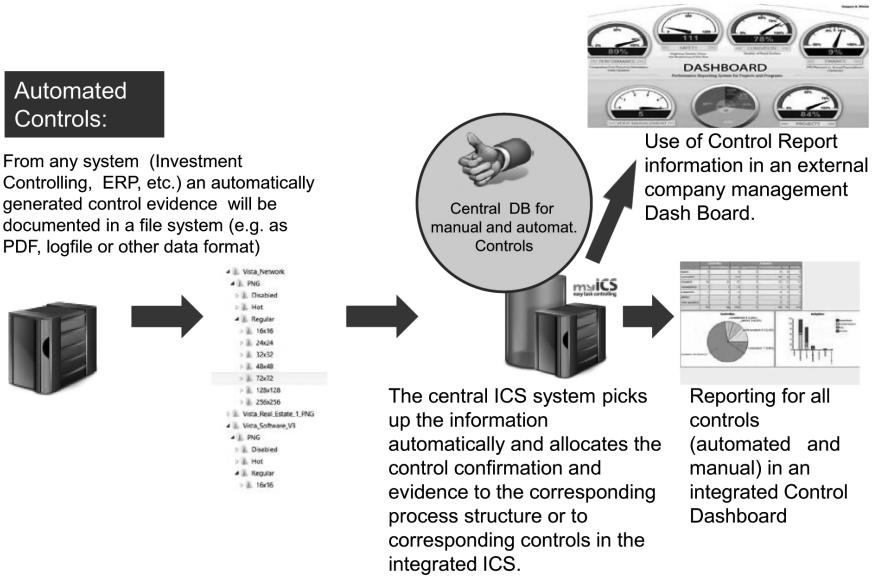

Figure 18.5 **Automated Controls in an Internal Control System.** This figure illustrates the reporting integration of automated controls in core systems with semiautomated and manual controls where control confirmation is performed by employees. *Source*: RFM Dr. Imfeld and myGRC/myICS Fecton GmbH.

Information Technology Support in Operational Risk and Control Processes

For IT support in the risk and control management process, one should test risk management concepts on standard office tools such as Excel. Once the maturity level of a risk and control concept is defined and the organization knows what should be implemented, the manager needs to consider standardized and more efficient IT tools that support the integration and automation of all manual and automated tasks and controls.

Some key requirements for IT support in the risk and control management framework for midsize financial institutions such as hedge funds are useful to make life easier in their risk and control management process:

- A web-based solution with decentralized access but a central database
- A modular structure supporting as a minimum expert risk assessments, control and mitigation processes, and a reporting functionality with a dashboard
- User-friendliness and easy handling of the IT tool for people involved in risk assessment and control activities across the company
- Automatic distribution of all reports, alerts, and tasks for controls and action items, processed on a defined scheduler (e.g., via an email function to an email program such as Microsoft Outlook)

- Automated sending out of control tasks based on defined frequencies and user groups, scheduled reports that are automatically updated on status and effectiveness of controls.
- A flexible representation of different structures such as organization, processes, or other structures such as product types, strategy types, or client segments
- An easy interface to an existing process documentation tool
- A flexible data management based on templates for standard controls or risks that allow simple copy-and-paste functions will support straightforward rollout of risk and control management processes in departments or subsidiaries without starting from scratch
- A dashboard report with integrated perspective on all risks and controls, automated or manual, by process and control status
- A very basic workflow support, complete and auditable data history, and a granular role and user rights concept
- Integration of automated controls and manual controls combined in a joint report on the status and effectiveness of all controls and mitigation measures

The solution should also allow growing along a maturity concept for the risk management. Three to five years may be needed for a concept's full rollout. Midsize and smaller organizations may also consider an outsourced IT solution combined with content-related support on risk management.

Summary and Conclusions

A key element for success is to start ORM within a well-defined framework. Main elements of such a framework are (1) a clear risk concept (possibly combining risks and chances), (2) a risk policy, (3) the risk management process, (4) roles and responsibility, (5) organization, (6) methods and instruments, (7) IT solution and risk communication.

- The risk policy should be defined in the beginning as a short, constitutional document in easy-to-understand language. It describes the main principles by which the organization manages its risks and very briefly mentions key elements of the framework to be set in place. The board should approve the risk policy.
- Ideally, risk management goals are driven by the company strategy. Aligning interest and incentives of managers to clearly defined goals occurs in the risk management process.
- A systematic risk management process should be set up with risk identification and assessment, risk mitigation, risk controlling, and finally risk strategy development. Ideally risks are identified across all processes in the organization with an end-to-end perspective along the value chain in the hedge fund business.
- Defining clear risk responsibility (commercial and legal risk responsibility) is essential, with line management and process ownership for the risk management function. Defining a maturity concept for the implementation and further development of risk management and its key instruments to be used is also essential. Starting small

and simple, but defining a clear road map in which direction the organization's risk management should go in the midterm future, for example, the next five years, is necessary.

- Qualitative and quantitative risk evaluation methods should be combined and too complex quantification exercises should be avoided in the beginning. Generating an enterprise-wide perspective on all risk categories with integration of operational risk scenarios into the market and credit risk analysis is important. Managers need to be aware that ORM is not just a one-time exercise, but a continuous improvement process that should manage identified risks not by reserving capital, but with the systematic establishment and control of documented risk mitigation measures and recurring risk controls. Outsourced processes should be included in the risk analysis. Whether the process is an in-house process or an outsourced process (e.g., support processes in HR, IT, and finance) is of less importance than the risk impact of failures in processes, systems, or errors of employees finally remaining on an organization's balance sheet.

For the IT support in the risk management process, managers should test risk management concepts first on a simple office tool such as Excel. Once the concept has been proven in a pilot case, the next step is 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.

Discussion Questions

1. Describe how the risk of using outdated antivirus software can be reflected in the hedge fund's risk management process.
2. Discuss the main methods used to identify operational risks in financial institutions such as hedge funds.
3. Explain how an organization can be assured that operational risks in outsourced processes are addressed and managed properly and according to an organization's standards.
4. Identify the key elements to include in an overview reporting dashboard on operational risk.

References

Bank for International Settlements. 2001. "Operational Risk, Consultative Document." Basel Committee on Banking Supervision. Available at http://www.bis.org/publ/bcbs86.htm.

Bank for International Settlements. 2009. "Results from the 2008 Loss Data Collection Exercise for Operational Risk." Basel Committee on Banking Supervision. Available at http://www.bis.org/publ/bcbs160a.pdf.

Bollen, Nicolas P. B., and Veronika K. Pool. 2009. "Do Hedge Fund Managers Misreport Returns? Evidence from the Pooled Distribution." *Journal of Finance* 64:5, 2257–2288.

Brown, Stephen, William Goetzmann, Bing Liang, and Christopher Schwarz. 2009. "Estimating Operational Risk for Hedge Funds: The ω-Score." *Financial Analysts Journal* 65:1, 43–53.

Brown, Stephen, William Goetzmann, Bing Liang, and Christopher Schwarz. 2012. "Trust and Delegation." *Journal of Financial Economics* 103:2, 221–234.

CapCo. 2003. "Understanding and Mitigating Operational Risk in Hedge Fund Investments." White paper, Capital Markets Company.

Cassar, Gavin, and Joseph Gerakos. 2010. "Determinants of Hedge Fund Internal Controls and Fees." *Accounting Review* 85:6, 1887–1919.

Dimmock, Stephen G., and William C. Gerken. 2012. "Predicting Fraud by Investment Managers." *Journal of Financial Economics* 105:1, 153–173.

ORX. 2011. "Operational Risk Reporting Standards." Available at www.orx.org.

van der Aalst, Wil, Jörg Desel, and Andreas Oberweis. 2000. *Business Process Management: Models, Techniques, and Empirical Studies.* New York: Springer Verlag.