

**Deloitte.**

Institute of Insurance Economics



University of St.Gallen

# Management of Operational Risks in Insurance

Current situation, trends and benchmarks when dealing with operational risks

Deloitte & I.VW-HSG  
June 2007



Audit • Tax • Consulting • Corporate Finance •



# Contents

Table of figures	2
Preface	3
Key findings	4
Study concept	5
1. Driving factors of operational risk management	7
2. Risk policy and strategy	10
3. Risk identification and classification	13
4. Risk management process	18
5. Reporting	23
6. Risk governance and risk organization	26
7. Integration of ORM into enterprise risk management (ERM)	29
8. Way forward	31
9. Focus on Switzerland	32
10. Conclusions and outlook	34
Authors and contacts	36

# Table of figures

Figure 1:	Overview information of the companies is included in the survey sample	5
Figure 2:	Study structure	6
Figure 3:	Country-specific identification of the main reasons for managing OpRisk	7
Figure 4:	Strategic reasons and ability to assess damage potential	8
Figure 5:	Origin of ORM initiative	9
Figure 6:	Typology of OpRisk policies	10
Figure 7:	Basic strategies for managing OpRisk	11
Figure 8:	Strategic concept and typology of OpRisk policy	11
Figure 9:	Share price loss after an operational event, Banking vs. Insurance industry	12
Figure 10:	Basis of risk definition and classification as a function of ORM	13
Figure 11:	Definitions of OpRisk	14
Figure 12:	Three classification levels of OpRisk within the framework of Basel II	14
Figure 13:	OpRisk consideration levels	15
Figure 14:	Main risk categories of OpRisk definition	15
Figure 15:	Most important operational risks of companies by country	16
Figure 16:	OpRisk with the biggest actual losses in relation to those perceived as important	17
Figure 17:	Status quo of ORM sub-processes	18
Figure 18:	Tools and methods for OpRisk identification	19
Figure 19:	Tools and methods for OpRisk assessment	20
Figure 20:	Quantitative assessment methods to be employed in the future	20
Figure 21:	Annual damage potential from OpRisk	21
Figure 22:	Frequency and order of magnitude of operational losses in the insurance industry	22
Figure 23:	Form of external reporting	24
Figure 24:	Frequency and recipients of internal OpRisk reporting	24
Figure 25:	Current and planned ORM functions	26
Figure 26:	Existing ORM functions	27
Figure 27:	Future ORM functions	27
Figure 28:	Other organizational units participating in ORM	28
Figure 29:	ORM as part of ERM	29
Figure 30:	Extent of risk aggregation	30
Figure 31:	ORM areas capable of improvement – mean value	31
Figure 32:	Basis of risk definition and classification in Switzerland	32
Figure 33:	Quantitative assessment methods/tools to be employed in the future in Switzerland	33

# Preface

Globalization as well as technical, political and social changes are resulting in insurance companies being increasingly exposed to greater and more complex risks. Thus, to successfully operate in the market, insurers are being compelled to take considered and controlled risks. Consequently, their need for active risk management is increasing.

Within the framework of active risk management, the subject of “operational risks” (OpRisk) is increasingly growing in relevance for insurance companies. In addition to new value-adding strategies, such as outsourcing/offshoring or the necessity of comprehensive risk management in terms of Enterprise Risk Management (ERM), there are first and foremost regulatory demands (e.g. Solvency II, Swiss Solvency Test and the Sarbanes-Oxley Act), which require to manage this risk category. These legal regulations are at present in the initial stages of development and have partially still not been specified in detail with regard to concrete requirements. For numerous insurance companies, the resulting leeway with reference to the development of Operational Risk Management (ORM) thus leads to the need for intensive and detailed contemplation and discussion around the subject of OpRisk.

During the course of these developments, insurers will be faced with the following questions:

- What driving factors led to the introduction of ORM?
- What is the understanding of OpRisk?
- What components of the ORM framework have been implemented and how are responsibilities assigned?
- What developments can be expected and where is potential for improvement?

The present study will provide positive answers to these questions. Furthermore, the results serve to derive recommendations for action by management. The study serves as a contribution to the discussion and provides knowledge with regard to OpRisk in the German-speaking insurance sector.

We would like to thank all those who, by their participation, contributed to the success of this study.



Dr. Daniel Kobler

Strategy & Risk Consulting  
Financial Services Industry  
Deloitte



Prof. Dr. Hato Schmeiser

Director  
Institute of Insurance Economics of the University of St. Gallen

# Key findings

This study was produced with the support of 54 companies in Germany (D), Austria (A) and Switzerland (CH) by the University of St. Gallen's Institute of Insurance Economics (I.VW-HSG), in collaboration with Deloitte. Starting from the driving factors leading to the introduction of ORM, it explains how the insurance industry assesses its current state of development and its requirements with regard to ORM (policies/strategies, definitions and categories, processes, reporting, governance and organization), as well as its integration into a company's overall Enterprise Risk Management (ERM) framework.

The study shows that, although the majority of insurance companies cannot conclusively determine OpRisk damage potential, they have, however, clearly recognized the dangers. Hence, ORM in the German-speaking insurance sector is today mostly being set up.

## Ten key findings of the study

1. The main reasons for introducing ORM are regulatory guidelines, the need for a comprehensive view of risk (in connection with establishing company-wide ERM systems) and protection from OpRisk-related losses.
2. Most of the insurers surveyed have an elaborated risk policy and philosophy. Only a third of these, however, have concretized this into strategies for OpRisk management.
3. The majority of the insurance companies use the Basel II banking standard for the definition and classification of OpRisk.
4. Operational risks are assessed differently in A, CH and D, but legal and political risks, IT risks, inadequately defined processes and the turnover of key personnel are, without exception, assessed as critical.
5. Whereas "classic" elements in the risk-management process (communication, reporting) are considered to be well implemented by a majority of those questioned, systematic loss-data collection, an essential basis for overall ORM, is rarely carried out. Two thirds of those questioned do not consider themselves in a position to assess their annual OpRisk losses.
6. Internal OpRisk reporting is carried out by all those questioned. For half of them it is part of the internal controlling system. The vast majority of those questioned have also established external reporting.
7. The majority of companies have at least one ORM function. In two thirds of the cases, overall responsibility lies with management or the CEO.
8. The observed inadequate institutionalization of ORM is also related to the fact that a wide range of organizational units, in different roles, are involved in the process.
9. The companies in the survey identified the need for action as being moderate to high in all the ORM areas, whereas the building up of OpRisk data collection and the increase of risk quantification was mentioned most frequently.
10. For insurance companies in Switzerland, in comparison with Germany, ORM is still in its infancy, with regulatory guidelines being the primary driving factor. The institutes concerned have recognized additional requirements for implementation.

# Study concept

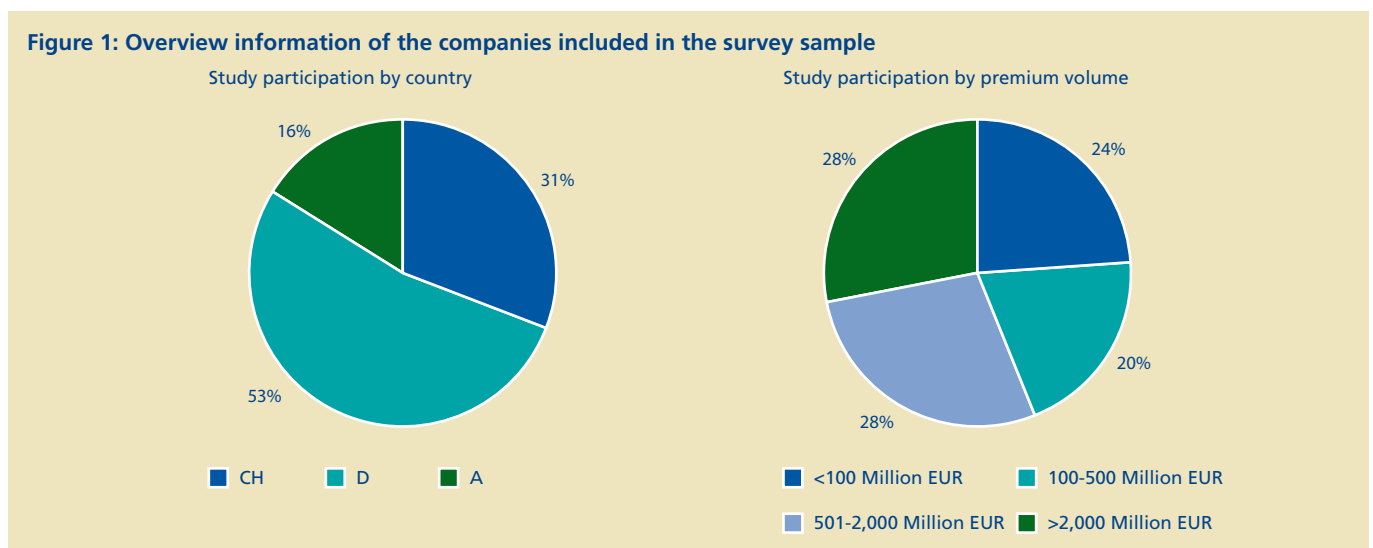
## Objectives of the study

The study identifies the understanding and characteristics of, and trends in the management of operational risks in the Swiss, German and Austrian insurance industries. Based on a large-scale survey of executives and specialists in the branch, and against the background of increasing regulatory demands, aspects concerning the concrete implementation and integration into companies were first of all solicited. In particular, ORM definitions, organizational implementation/processes, reporting and governance were covered.

By summarizing and comparing the individual opinions in this survey, areas of consensus and dissent within the industry become visible. This offers the individual companies a grid for positioning their organization and a possibility for benchmarking. The study thus serves both as a checklist, in order to close gaps, as well as to point out ideas for differentiation in the market.

## Methodology and random sample

The present study is the result of a joint investigation by Deloitte and the Institute of Insurance Economics of the University of St. Gallen (I.VW-HSG). The questionnaire was based on the results of relevant research work, and was completed by means of focused in-depth interviews. The survey was carried out in Switzerland, Germany and Austria from June to September 2006. In total, 54 companies participated. This corresponds to a response rate of 47%. 53% of the participants were from Germany, almost a third from Switzerland, and 16% from Austria. In Switzerland, half of the companies contracted participated in the survey (figure 1).

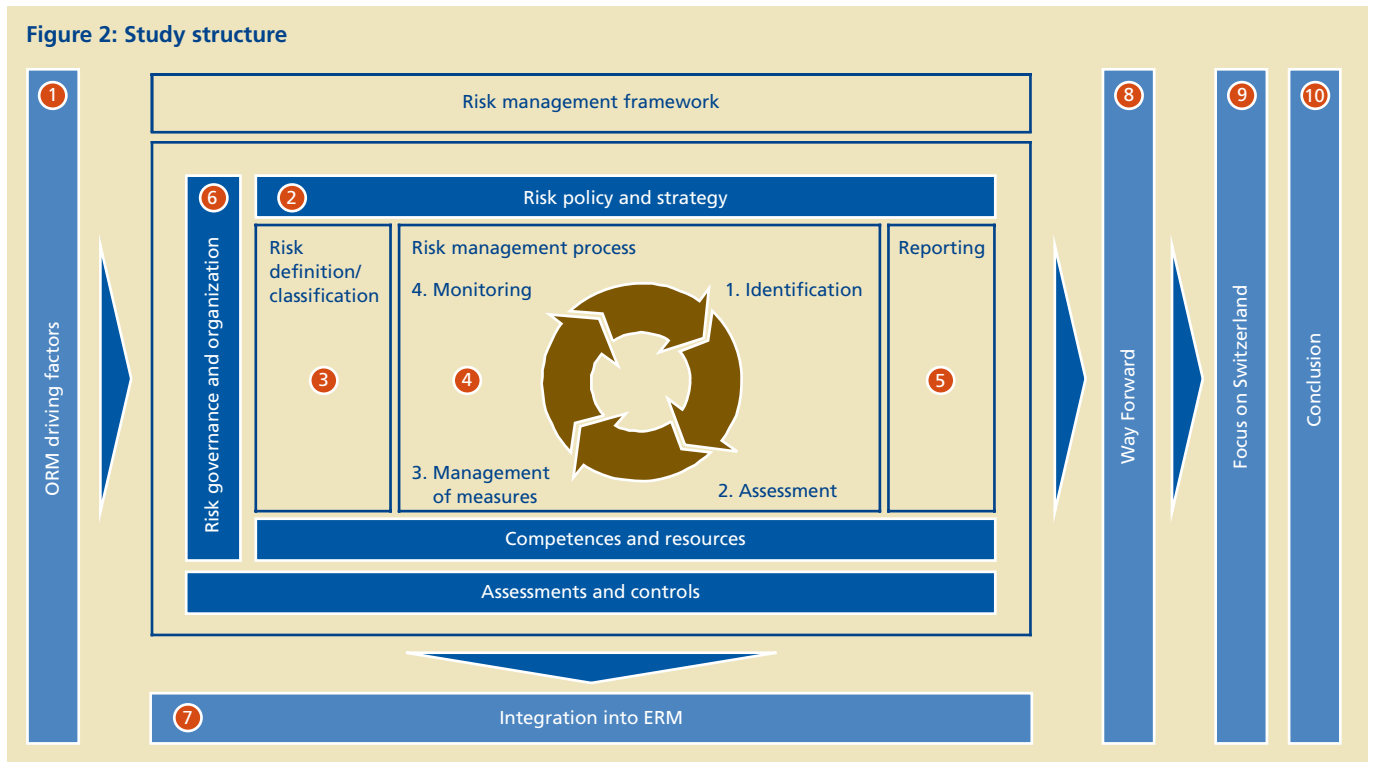


More than half the participants came from companies that had a premium volume of EUR 500 million or more. 10% of the companies responding are active in pure life insurances and 20% in pure non-life insurances. Most of the companies are thus active in both lines of business. The study also took reinsurance and health insurance companies into consideration.

Compared with Germany and Austria, Switzerland has an above-average share of large insurance companies. This was also reflected in the study, where the average number of employees in the companies surveyed was 4,126 in Germany, 6,338 in Switzerland and 2,195 in Austria.

Setup and structure

The definition of a suitable overall framework forms the starting point for implementing structured and efficient risk management. The study analogously follows the structure of an operational risk management (ORM) framework<sup>1</sup>, and, therefore subdivided into 10 chapters (figure 2).



Chapter 1 deals with the fundamental driving factors for ORM from today’s point of view. Based on the observable motivation in the past, the current situation is examined and corresponding needs for action derived.

The survey results for the seven building blocks of the ORM framework follow in chapters 2 to 6. Systemized risk management requires the definition of a risk policy and strategy which is adapted to the needs of the specific company (chapter 2). This is operationally implemented in the company via the elements risk definition and categorization (chapter 3), risk-management process (chapter 4) and reporting (chapter 5). The risk strategy is supported by a clear risk organization and risk governance (chapter 6), which includes all areas of risk management.

Chapter 7 deals with today’s situation and the further development of integrating ORM into a complete enterprise risk management (ERM) framework. In chapter 8, the results of the survey are highlighted with regard to the perceived future development potential in ORM. Chapter 9 summarizes the results from the Swiss perspective. The conclusions of the study are presented in chapter 10.

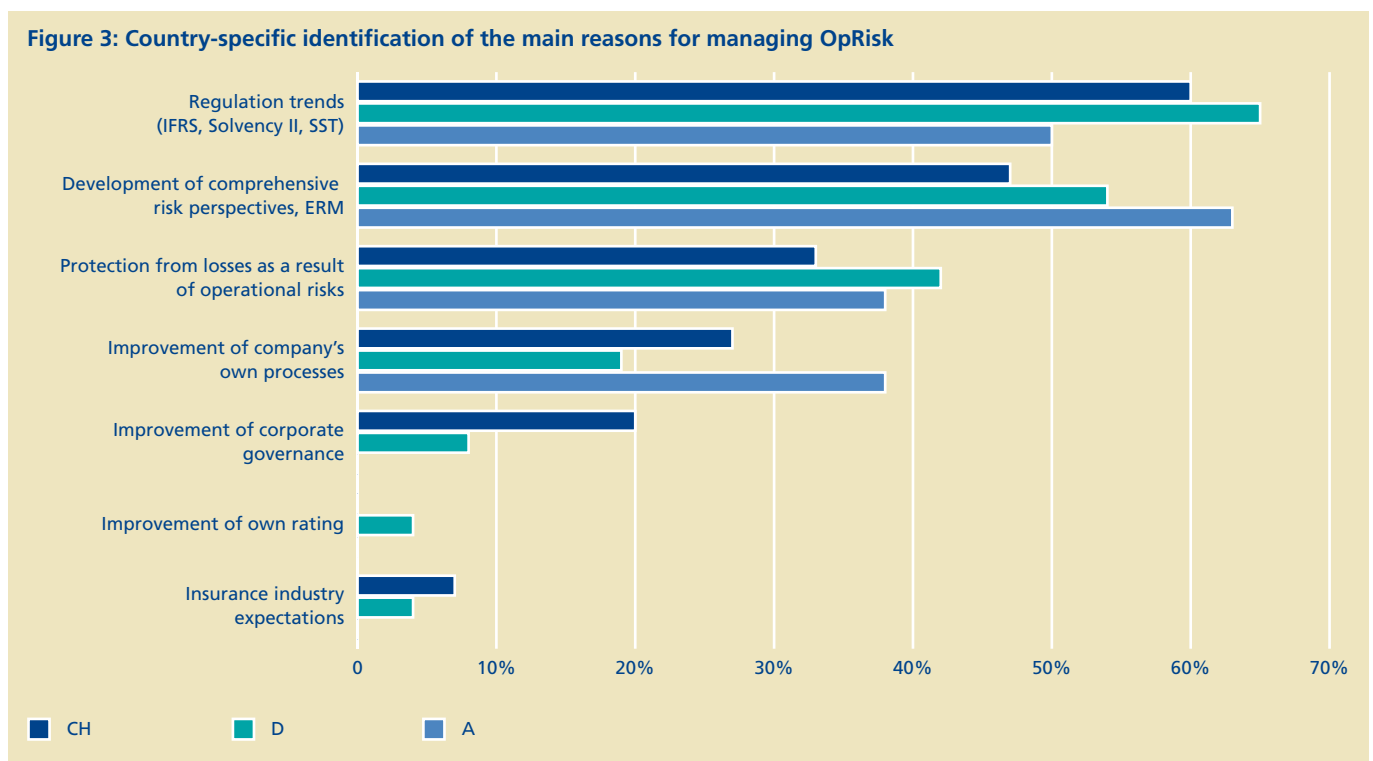
<sup>1</sup> A framework encloses all aspects that have to be considered in a risk system (e.g. strategy, process, quantification model, etc.). In addition, the interaction of the various elements can be represented as a model in order to obtain a complete overview of the risk system.



# 1. Driving factors of operational risk management

Dealing with risks arising from operational activities, for instance, as a result of imperfect processes or dishonest employees, is not a new topic for insurance companies. Company crises, however, have reinforced the opinion of supervisory authorities and financial service providers that OpRisk has to be thoroughly and centrally controlled, and should constitute an integral part of ERM.

In this context, external and internal factors led the insurance companies surveyed to develop and introduce ORM (figure 3).



## Increasing regulation

For the vast majority of companies, the main reason for introducing ORM is growing regulatory demands. In Europe, the focus is on the Solvency II regulations<sup>2</sup>. Besides financial securitization in the 1st pillar, OpRisk are part of the supervisory screening process and risk management of the 2nd pillar and of the transparency regulations of the 3rd pillar. These regulations only exist in the form of proposals and are not to be reckoned with before 2009, with the introduction of Solvency II. The new Swiss insurance-supervision law should also be taken as an example. This anticipates many of the developments of Solvency II and includes the first requirements of ORM<sup>3</sup>.

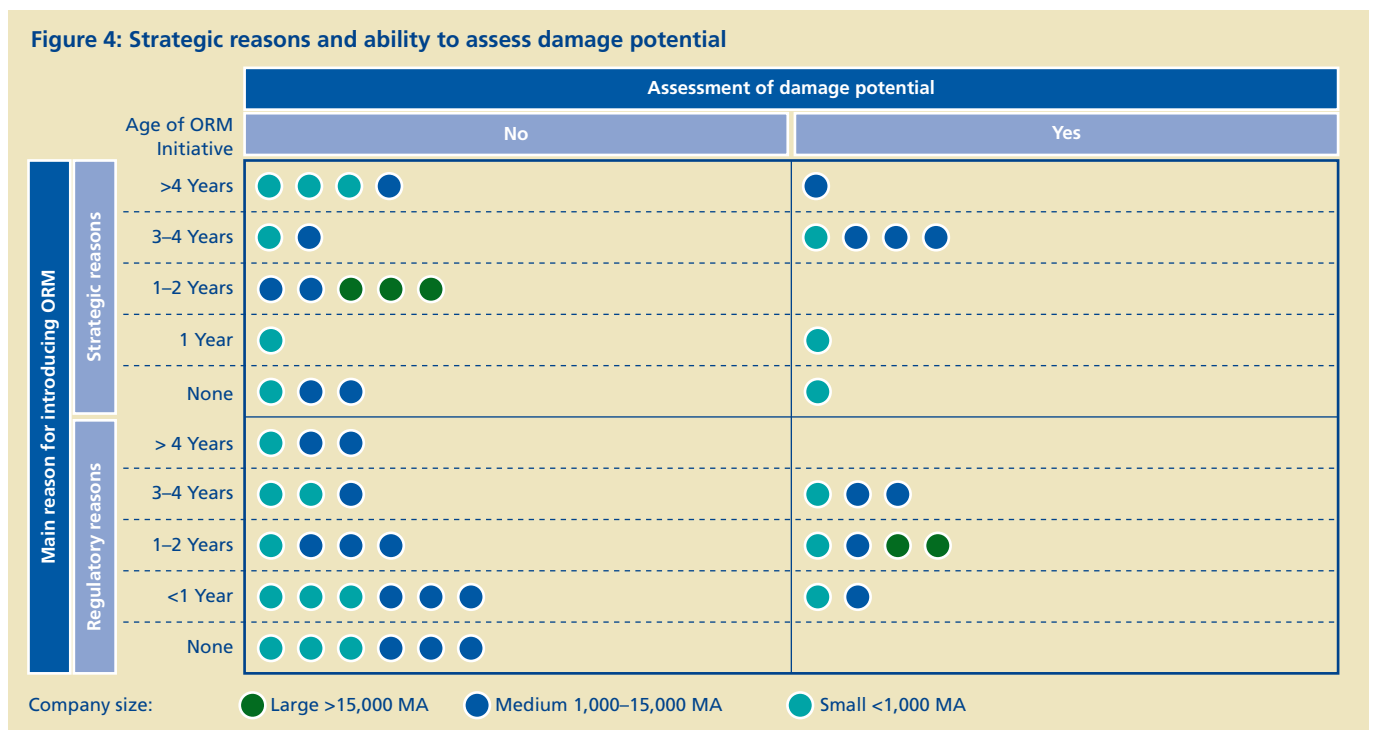
<sup>2</sup> Within the framework of "Solvency II", a complete revision of the current regulations of insurance companies is planned. The objective is to protect insurance-policy holders fairly in all the EU member states and to put in place competitive conditions within the sector (source: European Commission).

<sup>3</sup> Since 1/1/2006, Swiss insurance companies have been obliged to record and assess OpRisk, and to report the results periodically to the supervisory authorities. Furthermore, it is planned from the supervision side to introduce regulations for financial securitization as soon as OpRisk can be quantified. In particular, with the coming into force of Art. 98 of the Swiss Supervision Ordinance (AVO), in the future, insurance companies will not only be compelled to record and assess operational risks on their own responsibility, but the regulator will additionally demand the acquisition and analysis of loss data as a basis for quantification.

**Comprehensive risk perspective and other factors**

The desire for a comprehensive risk perspective, respectively the completion of ERM around OpRisk represents another very important driving factor for the introduction of ORM. Protection from losses as a result of OpRisk events is named in third place only, which for many companies must also be seen in connection with the lack of ability to quantify these losses. Thus, what is central to actuarial and financial market risks, namely the avoidance of costs, is not once named as the trigger by 40% of the participants. Further, ORM is regarded as a process improvement tool for quality control and continuous process improvement. Likewise, the assessment of rating agencies, which increasingly assess companies from the point of view of adequate risk management, is cited as a reason. Reputation risks are not mentioned as ORM driving factors. If the individual countries are compared with the overall result, only slight differences can be detected. Only in Austria is the development of a comprehensive risk perspective cited more often than the regulation trend.

As a consequence of these various demands on ORM, there is an increasing need for action. In this context company development stages vary. Figure 4 below illustrates the difference between insurance companies where ORM was introduced for regulation reasons and those where it was introduced as a strategic intention.

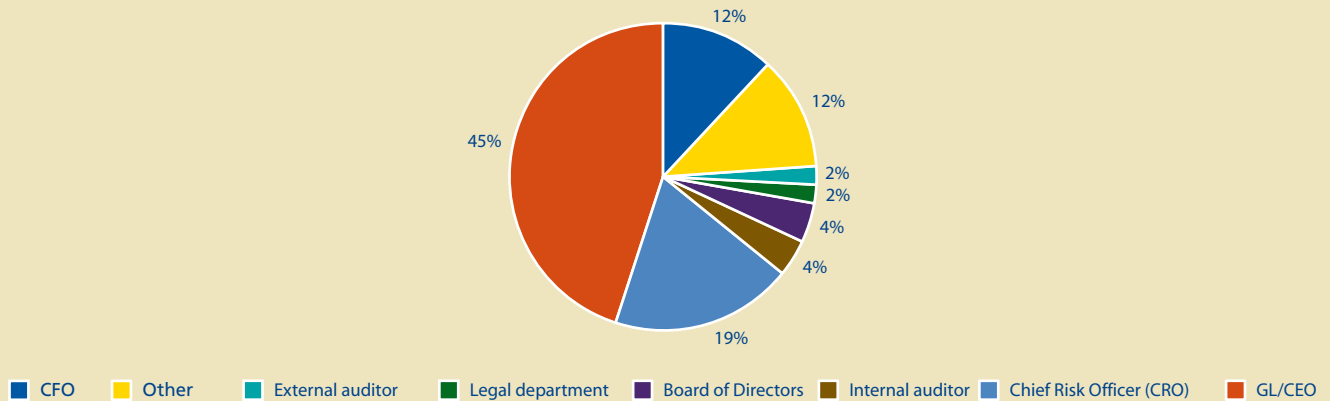


The strategic value of ORM, such as the improvement of a company's own processes or compliance with corporate governance, is assessed more highly by those companies who have already had an ORM strategy for a long time (Figure 4). In addition, these companies are able to better assess the damage potential of OpRisk. The emphasis on strategic reasons for the introduction also primarily correlates with the "age" of the initiative.

In contrast to groups with advanced ORM, there are numerous small- and medium-sized companies (almost 40%) where the ORM initiative is less than a year old, and these primarily see it as a regulatory obligation. This shows that the growth of regulations was the primary contributing factor for the introduction of nascent ORM initiatives. Since internal driving factors are of little relevance in these cases, no, or only few, tools for determining damage potential have been developed thus far, which is why effective risk assessment, or even securitization with own capital, is impossible.

Strategic processes, if existing, were started by management or the CEO in almost half the cases. CFOs and CROs played a decisive role in a further third of the companies interrogated. Other initiators, such as external auditors, internal auditors, board members or supervisory board members were mentioned only rarely, as also was the open category "Others", where sporadically the parent company or the controlling department were named as the prime movers (figure 5).

Figure 5: Origin of ORM initiative



When sorted by country, no major differences were identified with regard to this question. Only in Switzerland does the impetus for ORM come somewhat less frequently from management/CEO, but rather from the CRO or internal auditing. However, the size of the insurance company surveyed certainly plays a decisive role.

In the two smaller categories, <500 and 500 to 2000 employees, the activity was started by management or the CEO in most cases. For larger insurance companies, this only applies in a third of the cases, since there, the CFO (or the CRO) and occasionally the external auditor were the prime initiators.

**Intermediate conclusion**

- The main reasons for introducing ORM are regulatory pressure, the need for a comprehensive risk overview and protection from OpRisk related losses.
- Companies with advanced ORM initiatives notably emphasize strategic reasons for ORM, whereas those with more recent processes are more likely driven by regulation.
- Management attributes a high degree of attention to strategic ORM initiatives and management or the CEO initiates them in most cases.

## 2. Risk policy and strategy

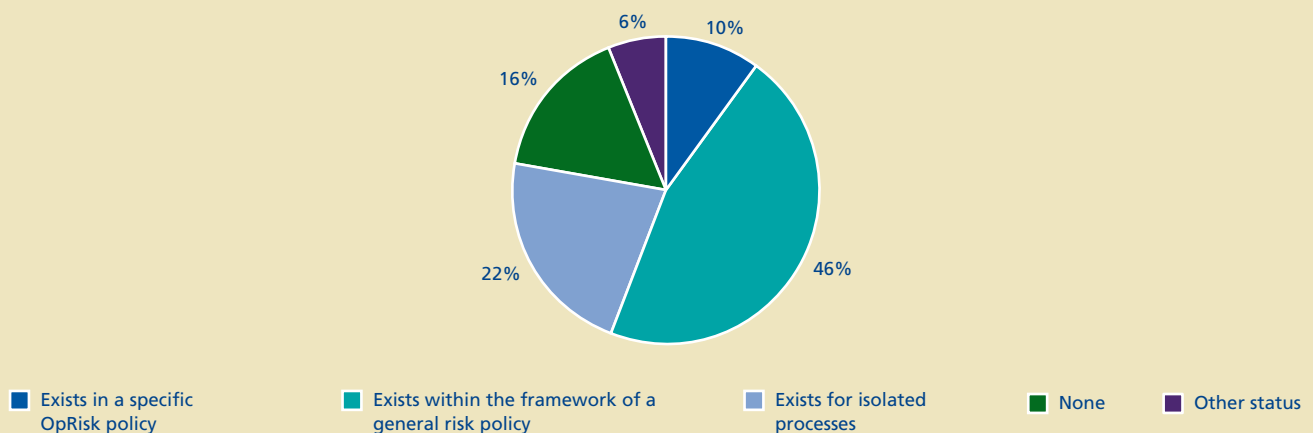
### Risk policy for managing operational risks

An operational risk policy (OpRisk policy) is the foundation for institutionalized management of operational risk. It serves as a thinking and orientation framework, in order to better integrate existing approaches and tools when dealing with operational risks in companies. In terms of the management of operational risks, the risk policy must, amongst other things, fulfil the task of establishing the following guidelines:

- The definition of a decision criterion (success measure), enabling risk and return to be weighed up.
- The introduction of an upper limit for the magnitude of risk of a company.
- The definition of the extent of own capital as potential for covering risk, derived from the aspired rating.
- The establishment of operational risks deemed unavoidable from the insurance companies' point of view, as well risks which should normally be transferred, taking the related costs into account.

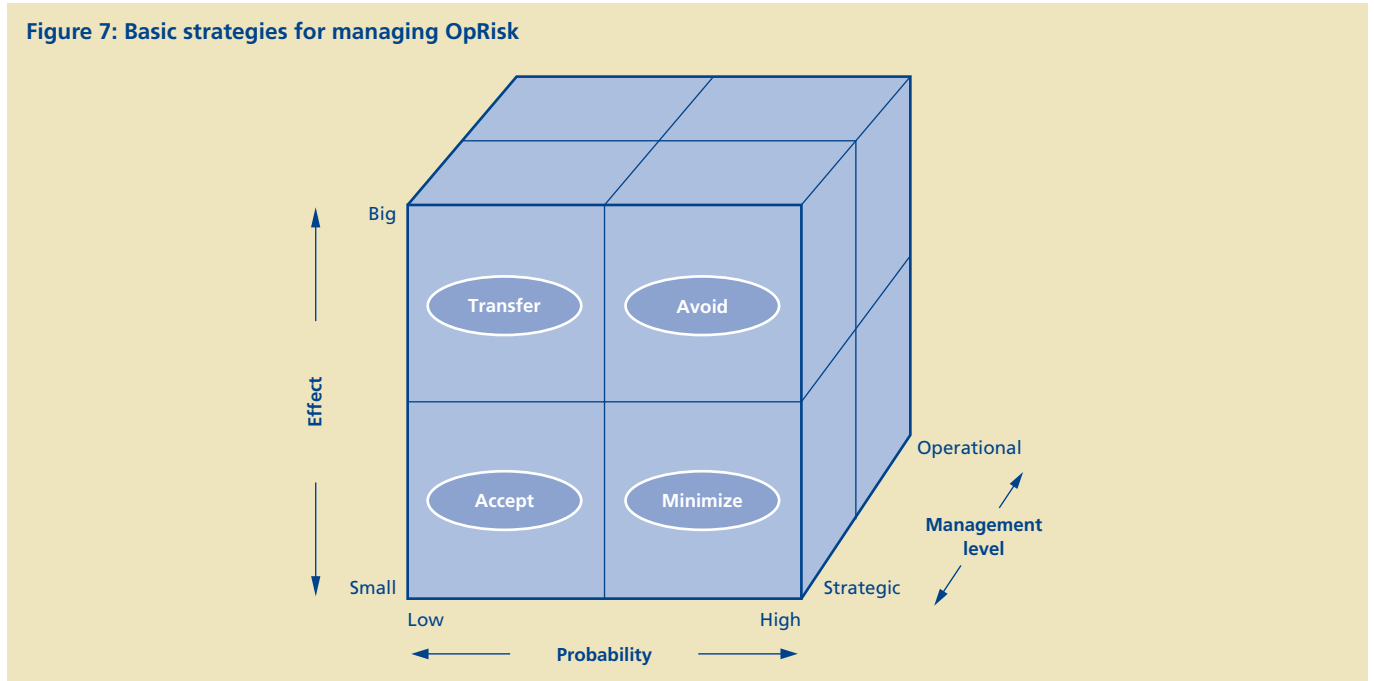
84% of the companies questioned within the framework of this investigation have a risk policy that also covers OpRisk. However, of these, most do not have a specific OpRisk policy, but instead only cover this kind of risk within the framework of a process-oriented or general risk policy. A mere 10% of the insurance companies, in general those with more than 10,000 employees, have a specific OpRisk policy. Over a quarter of the smaller companies (<500 employees) have not yet implemented any policy. It becomes clear that, for many companies, more intensive consideration of this topic will still only become a necessity in the coming years (figure 6).

Figure 6: Typology of OpRisk policies



**Basic strategies for managing OpRisk**

In the management of OpRisk, the following four action alternatives, referred to as elementary, are often defined, dependent on probability and the expected effect of a risk: accept, minimize, avoid and transfer (figure 7).



In practice, these strategies are not to be considered only as action alternatives in the strategic sense, but, according to the decision level where they are used, they can also be operative measures or packages of measures within the framework of normal business risk management. With far-ranging measures, such as the outsourcing of IT or the sale of a complete business sector, that have significant influence on the risk potential of an insurance company, it would not be unreasonable to speak of actions of strategic importance and consequently also of a risk management strategy.

Within the framework of managing OpRisk, specific measures or packages of measures that focus on defined sections of an organization are regarded as distinct or special strategies. They are thus not an addition to the described elementary action alternatives, but concrete shapings of these. In practice, examples frequently seen are: disaster recovery, business continuity planning and outsourcing.

**Figure 8: Strategic concept and typology of OpRisk policy**

		Typology of OpRisk policy				
		None	Isolated process policy	General risk policy	Specific risk policy	
Main reason for introducing ORM	Strategic concept	>4 Years	●	● ● ●	●	
		3-4 Years	●		● ● ● ●	●
		1-2 Years	●	●	●	● ●
		<1 Year	● ●			
		None	●	●	● ●	
	Regulatory reasons	>4 Years	●	●	●	
		3-4 Years	● ●		● ● ● ●	
		1-2 Years	●	● ●	● ● ● ●	●
		<1 Year		● ● ●	● ● ● ●	●
		None	● ●	● ●	● ●	

Company size: ● Large >15,000 MA    ● Medium 1,000–15,000 MA    ● Small <1,000 MA

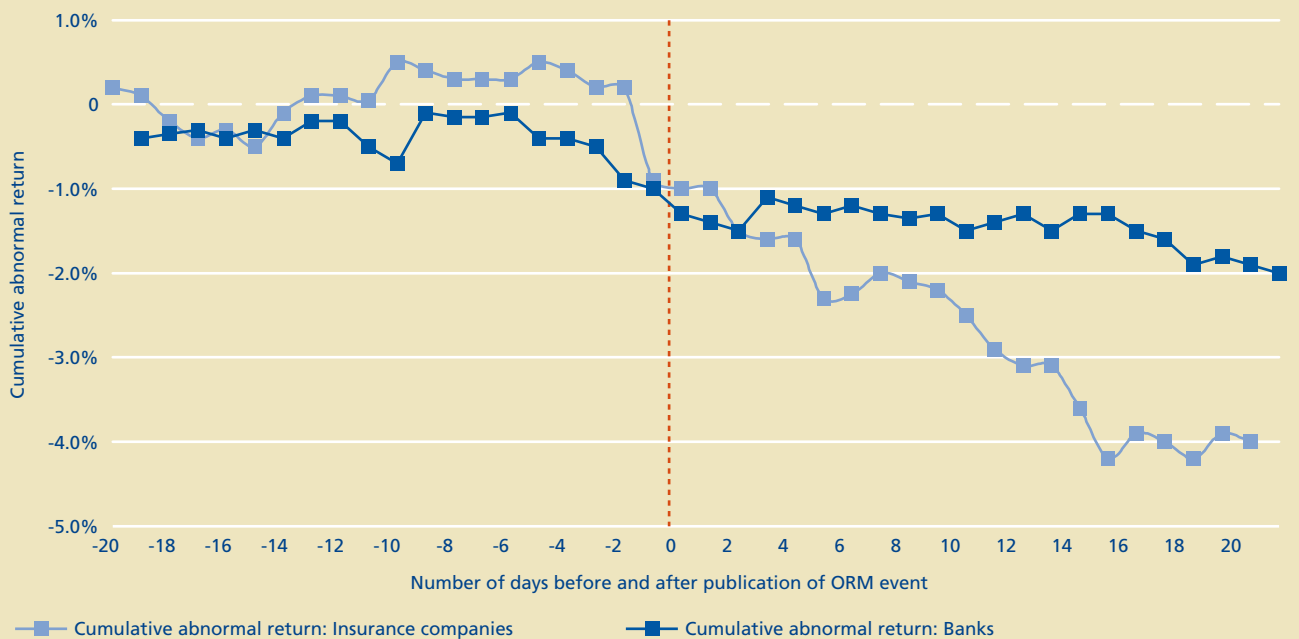
## Management of Operational Risks in Insurance

It is worth noting that of the 84% of companies surveyed that have an OpRisk policy, only about a third convert them into basic strategies for the management of OpRisk. However, only by doing this can measures or packages of measures be effectively defined in order to genuinely increase the strategic value of the company's ORM. Within this cluster, these are above all medium-sized and small insurance companies that have already been addressing ORM for more than three years. The lack of a definition for basic strategies can thus be justified by the fact that OpRisk management is still a relatively young discipline and is thus not yet integrated into existing management structures in a non-overlapping way. The appropriate package of measures should then be taken based on a clearly defined ORM structure (figure 8).

When an OpRisk event occurs, as well as a respective financial loss, the lack of such a control mechanism can also entail a considerable share price movement, particularly in the case of listed insurance companies (cf. excursus).

### Excursus: Cumulative abnormal return for banks and insurance companies before and after an operational loss event

Figure 9: Share-price loss after an operational event, Banks vs. Insurance companies



The study "The Market Value Impact of Operational Risk Events for U.S. Banks and Insurers" examined the effect of operational events on the share prices of the companies concerned.

It determined that, compared to banks, OpRisk events at insurance companies led not only to higher average financial losses, but also to more considerable share price movements: On average, the share price of US insurance companies falls due to an operational event by 4.15% within the following 20 days. In contrast, the share price of US banks falls by a mere 2% after a comparable event. In addition, the reaction time in the US insurance sector after such an event lasts significantly longer than in the banking sector. The study also establishes that the financial consequences of an appreciable negative share price development even exceed the damages due to the OpRisk event (figure 9).

Source: Cummins, J. David, Lewis, Christopher M. and Wei, Ran, "The Market Value Impact of Operational Risk Events for U.S. Banks and Insurers" (December 23/2004)

### Intermediate conclusion

- Most insurance companies have a risk policy that also basically covers OpRisk.
- Only about a third of companies turn their risk policy into one for the management of operational risks by means of basic strategies or package measures.

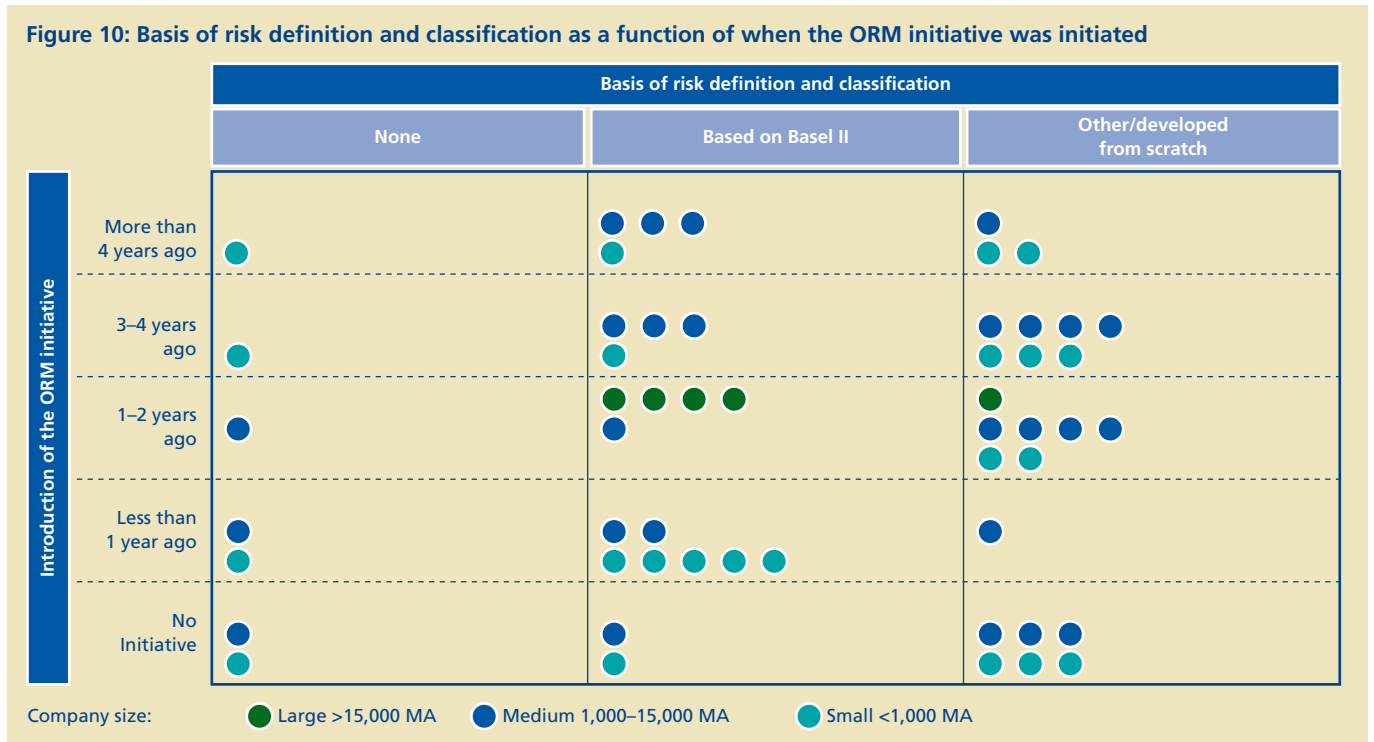
# 3. Risk identification and classification

An effective and efficient OpRisk management process with corresponding risk identification and assessment has to be based on a common understanding of OpRisk and clear risk classification. Definition and classification enable complete risk coverage and the definition of measures.

### Alignment on Basel II – for insurance companies too

In general, with regard to OpRisk definition and classification, insurance companies have aligned themselves to Basel II, even though the guidelines contained therein were originally developed for banks. This trend confirmed the investigation: 42% of the insurance companies cited Basel II as the basis used when contemplating OpRisk. With 26%, orientation towards a different basis was also popular. Only 19% of those questioned developed their OpRisk definition and classification from scratch, without using the support of an existing basis. In shape and form however, these differ widely from one another. One reason for aligning analogous approaches in insurance (such as Solvency II, Swiss Solvency Test) on Basel II is that bank rules and regulations have been available for some time already.

If an analysis is made according to company size (number of employees) and starting date of the ORM initiative, various tendencies in the selection of the basis for risk definition and classification become clear. Large insurance companies (>15,000 employees) in particular align themselves 80% to the Basel II standards. In contrast medium-sized companies (1,000 to 15,000 employees) have a strong tendency to use a different basis, either an existing one or self-developed. In the case of small- and medium-sized insurance companies, the initiation date of the ORM initiative even increases this tendency. However, smaller insurance companies (<1,000 employees), which only initiated the ORM initiative during the course of the previous year, tend to align themselves on Basel II (figure 10).



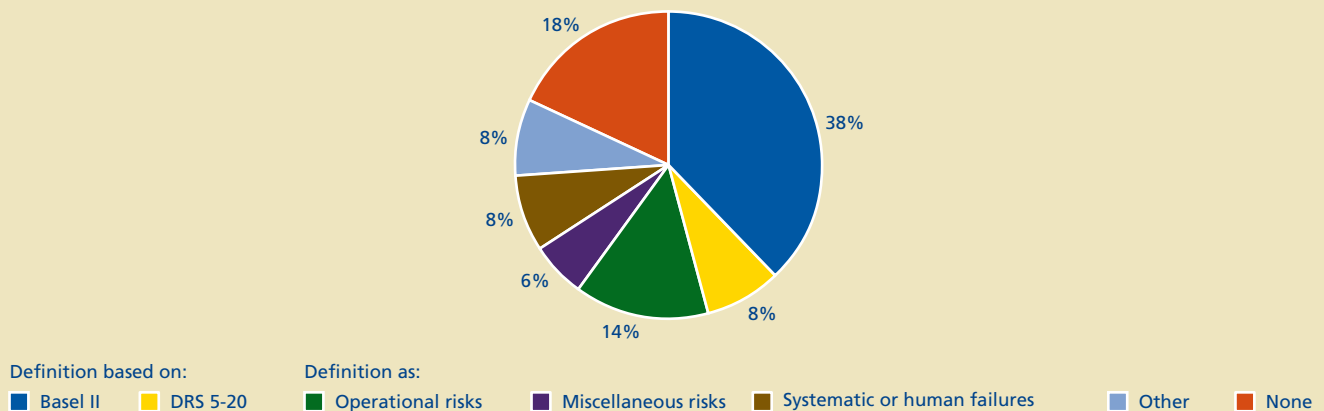
**Definition: Operational risk**

Against the background of this initial situation, it is not surprising that more than a third of the insurance companies surveyed define OpRisk according to Basel II (figure 11), namely:

“The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risks but not, however, strategic or reputation risks.” (Basel Committee for Banking Supervision, 2004)

A further popular basis, particularly for German companies, is the German accounting standard “DRS 5-20: Risk reporting for insurance companies”. It defines OpRisk as operational risks that result from human and technical failures or from external influencing factors. In addition, analogous to Basel II, legal risks which originate from contractual agreements or legal general conditions are also taken into consideration. The use of a miscellaneous OpRisk definition, in which all risks that cannot be classified in any other category are summarized, was only chosen by a few insurance companies. This fact should be seen as positive, since it has been shown in practice that a miscellaneous OpRisk definition frequently causes problems in delimitation and meaningful classification. Surprisingly, almost every fifth company surveyed indicated that it used no definition at all (18%). It must be concluded that, in these companies, ORM is only in the initial stages.

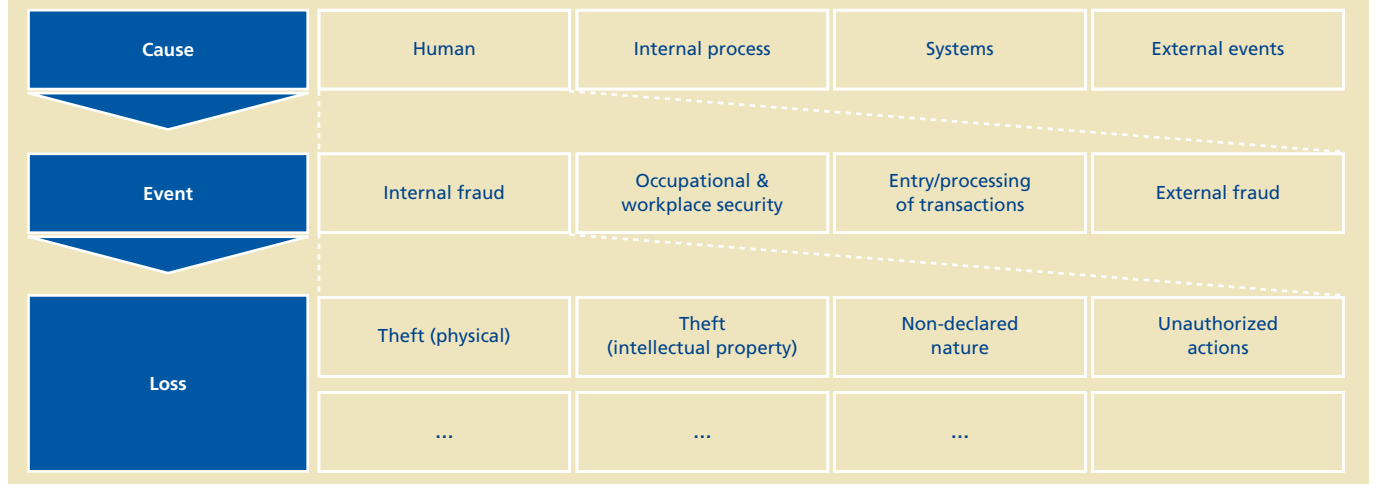
**Figure 11: Definitions of OpRisk**



**Classification of operational risks**

Based on the chosen risk definition/definition interpretation, in a next step, risk classification is derived. By way of example, figure 12 shows risk classification along the cause-effect chain, based on the definitions in Basel II:

**Figure 12: Three classification levels of OpRisk within the framework of Basel II<sup>4</sup>**

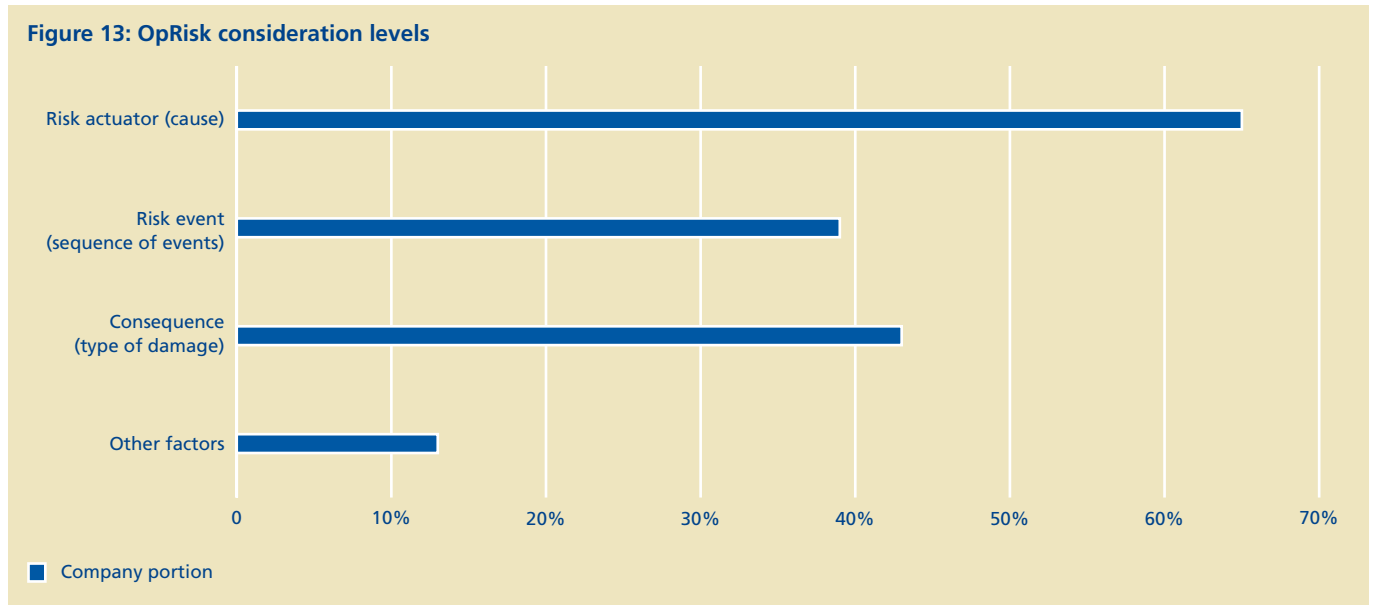


<sup>4</sup> Source: Basel Committee for Banking Supervision, “International Convergence of Capital Measurement and Capital Standards (Basel II)” (2004).



As shown in figure 12, Basel II divides OpRisk into categories entitled “Human”, “Internal processes”, “Systems” and “External events”, and assigns them to the corresponding risk events (second classification level). On a third classification level, losses are assigned to risk events and hence also to their causes. Thus, an optimum basis for the definition of adequate measures is created, which can be directly oriented towards fighting the cause or towards preventing the risk event. Potential damage or loss can thus be greatly reduced.

The study shows that two thirds of those questioned classify according to causes (figure 13). Only 39% of the insurance companies classified risks on the basis of risk events, whereas 43% of those questioned claimed to use the consequence of the risk event, i.e. the risk loss, as the classification criterion.

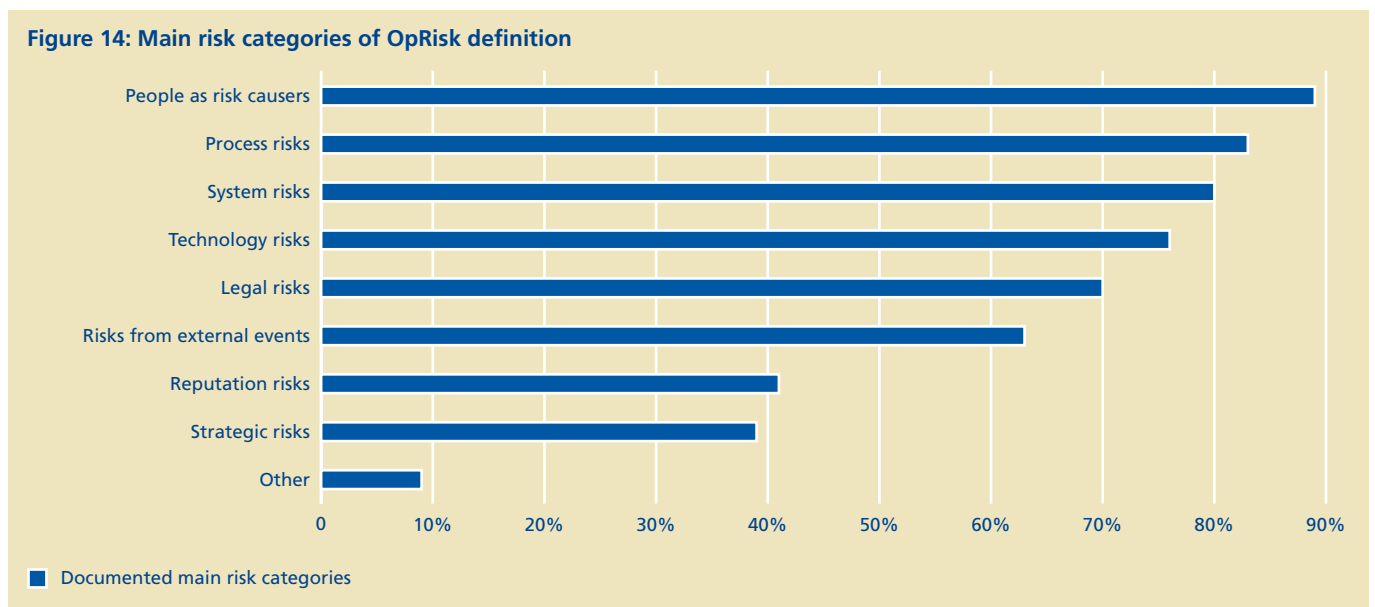


Altogether, less than half of those questioned (44%) give more than one registration criterion or have established more than one classification level. Only seven participants mentioned all three levels as relevant for their classification. This is independent of whether Basel II is used as the basis or not. Only 13% indicated that another classification criterion formed the basis of their classification.

This shows that, in the German-speaking region, there is still no consistent comprehensive classification of OpRisk. Wrong classification can, however, lead to false estimations with regard to damage potential and appropriate measures.

**Main risk categories in practice – 1st level “Risk causes”**

Based on the insurance company survey, figure 14 shows the breakdown in practice of the main risk categories currently used.



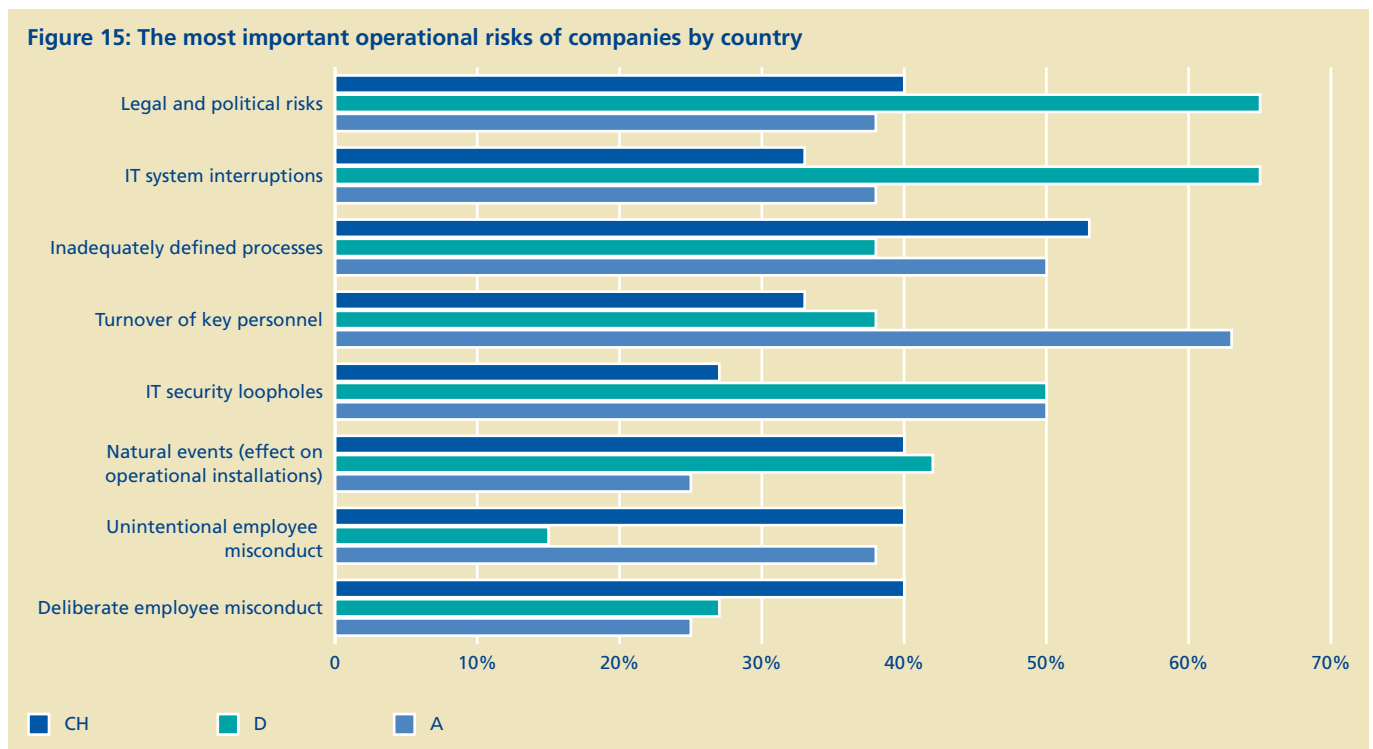
## Management of Operational Risks in Insurance

Three of the four suggested risk categories from Basel II, namely "Human", "Internal process" and "Systems" are, with 76 to 89%, used as the most important main categories by the majority of companies. "External events", the fourth category, is nevertheless still named as the main category in 63% of cases. With 76%, the main category "Technology risks" attracts also high attention. Basel II records these risks under "Internal processes" and "Systems". Unexpectedly, over 50% of the companies oriented in one way or another to Basel II consider either "Reputation risks" or "Strategic risks", frequently even both, as the main category under OpRisk, even though Basel II explicitly excludes them. However, the naming of these risk categories by those companies not oriented towards Basel II was significantly less.

Under "Other", individual risks were mentioned such as "Cultural and ethical risks", "Leadership and organizational risks" and "Sales risks". Interestingly, even companies without a specific OpRisk definition have a clear classification grid.

### Classification of risks on the 2nd level "Risk events"

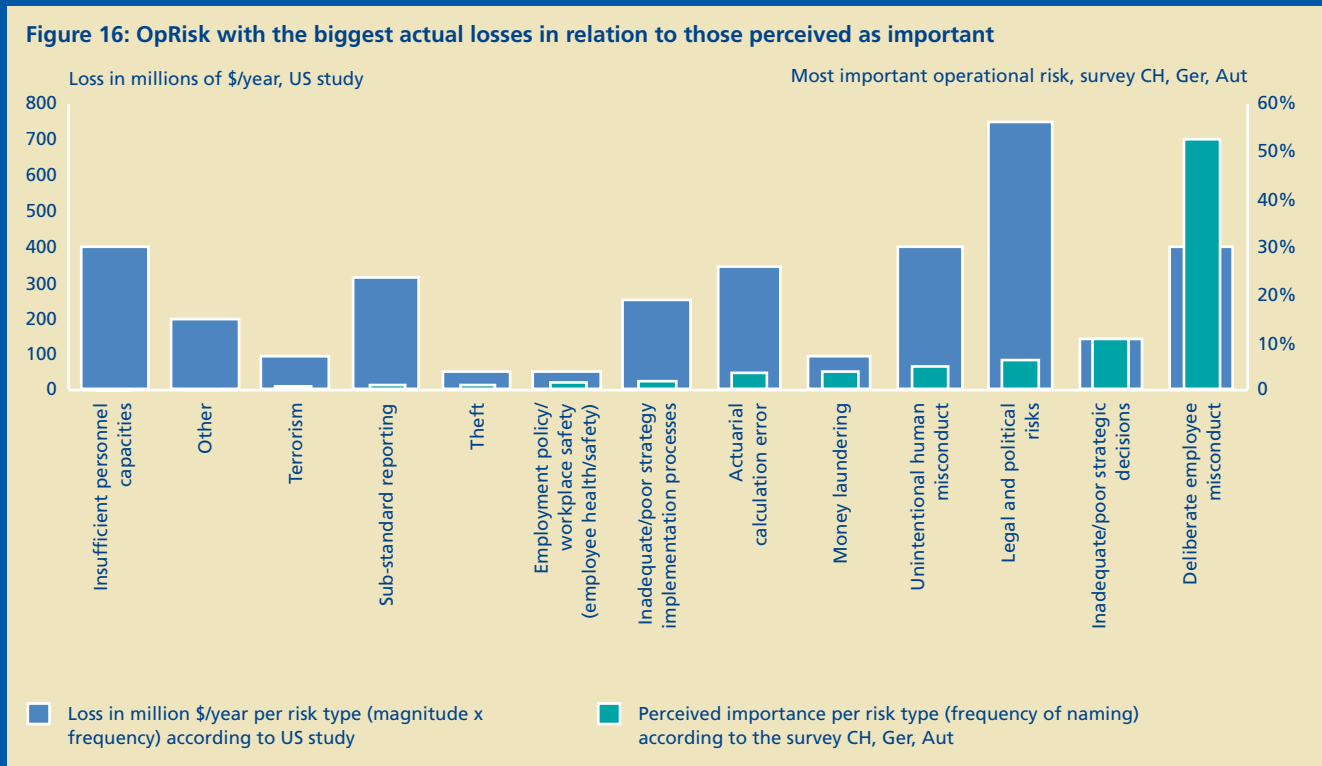
On the "Risk event" level, the companies questioned identified "legal and political risks", "IT system interruptions" and "inadequately defined processes" as OpRisk with the highest potential danger (Figure 15). While German companies see legal and political risks and IT matters as priorities, Swiss companies put the emphasis on inadequately defined processes and all kinds of employee misconduct. Detailed results show that while large companies particularly emphasize deliberate employee misconduct, small ones have to contend with employee turnover. Here, the necessity of systematic employee support and development is clear. In addition, it is apparent that small companies mention classification according to "Reputation risks" more than the average, whereas for large companies, the same is true for "Strategic risks". Furthermore, it appears that small companies in particular go into more detail with regard to their risk classification.



Based on the study, it can be seen that at the "Risk event" both technical risks, in particular IT risks, as well as soft factors, such as employee conduct, are important. This explains the wide spectrum that has to be embraced within the framework of ORM.

In the following excursus, effective, historically measured OpRisk losses are compared with the loss or potential damage assessment of the insurance companies. Since there is no such historical data for the German-speaking insurance branch in Europe, a US study was used. In view of this, country and market-specific differences in the interpretation of this comparison should be taken into account.

Excursus: Operational risk losses compared with risk assessment



In figure 16, the results of the present investigation were taken from the study “The Market Value Impact of Operational Risk Incidents for U.S. Banks and Insurers”. In it, the assessment of the importance of individual risks by the surveyed companies in CH, Ger and Aut were compared with the classification of actual incidents in the USA study.

Fundamental insights result from country-specific differences. Thus, in CH, Ger and Aut, “Deliberate employee misconduct” and “Inadequate/poor strategic decisions” are, for instance, rarely perceived, whereas these play a major role in the US study. In contrast, insufficient personnel capacity, sub-standard reporting and poor business calculations, as well as general human misconduct, are strongly perceived, but play less of a role in the analysis with regard to effective losses.

This discrepancy can be substantiated by the fact that, based on the first, less widespread, quantification of OpRisk, a purely intuitive weighting was frequently made, and thus relevant risks found only limited entry into the assessment.

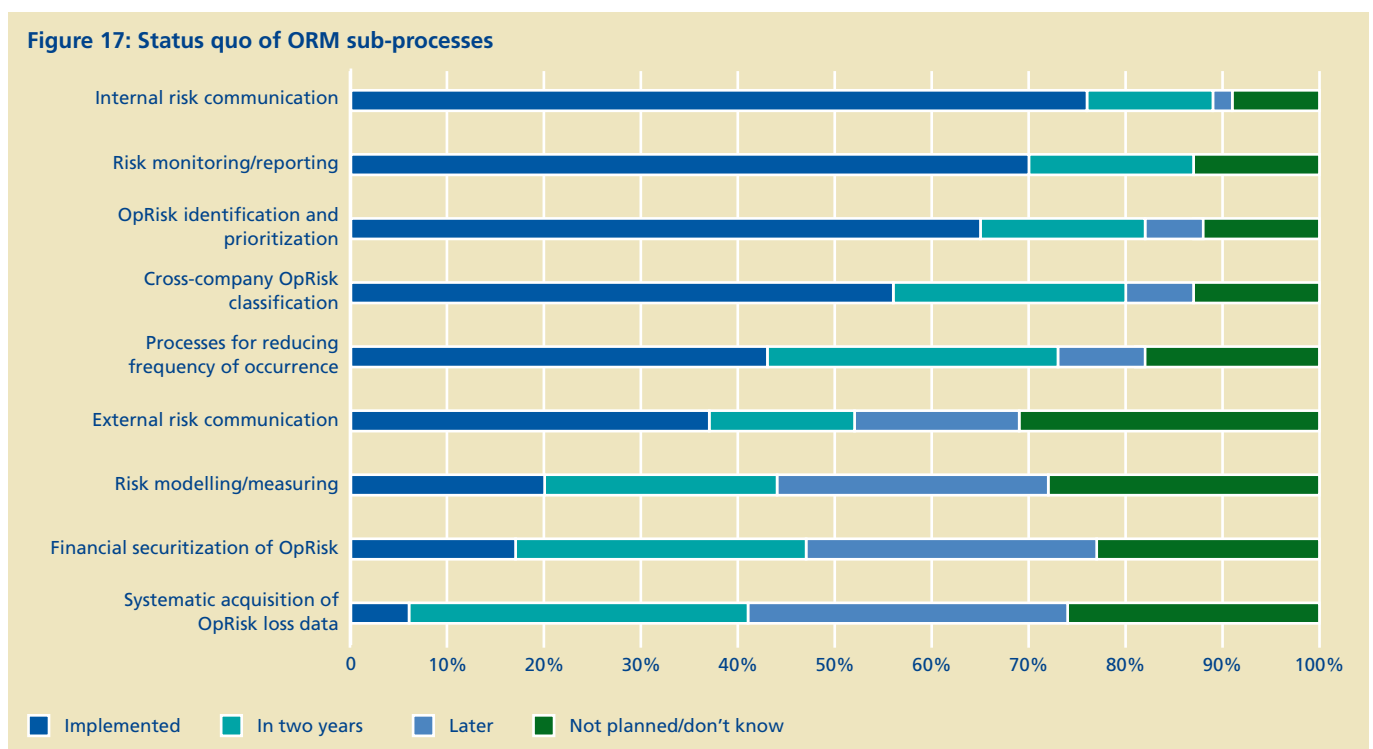
Source: Cummins, J. David, Lewis, Christopher M. and Wei, Ran, “The Market Value Impact of Operational Risk Events for U.S. Banks and Insurers” (December 23/2004)

**Intermediate conclusion**

- Basel II standards are also used by a large percentage of insurance companies for orientation with regard to the definition and classification of OpRisk.
- A multi-level, full classification according to the costs-by-cause principle (reason, event, loss) is still relatively rarely applied by insurance companies.
- Operational risks are assessed differently in different countries, with legal and political risks, IT risks, inadequately defined processes and the turnover of key personnel generally assessed as critical.
- The growing relevance of ORM in the insurance sector will, in future, lead to OpRisk definition and classification being increasingly adapted to the specific needs of insurance companies.

## 4. Risk management process

In the risk management process, classic process management matters, such as uniformity of definitions and clear communications, play an essential role. By the same token, the areas of risk identification, classification and assessment play a particularly key role. Since entrepreneurial activity is constantly changing, these process steps must follow steadily and in harmony with other control processes. With the regulation of suitable methods and indicators for risk identification, risk assessment and risk prioritization, data collection generally represents the biggest challenge. Data also has to be provided in a form suitable for appropriate analysis.



The survey showed that there were differences in the degree of implementation of the various ORM initiatives. Certain processes have for the most part been introduced, whilst others have been postponed to a "later" date. Such postponement can either be a consequence of prioritization or an illustration that the importance of the process is still unclear. In general, it can be assumed that the ORM systems are only in the start-up phase.

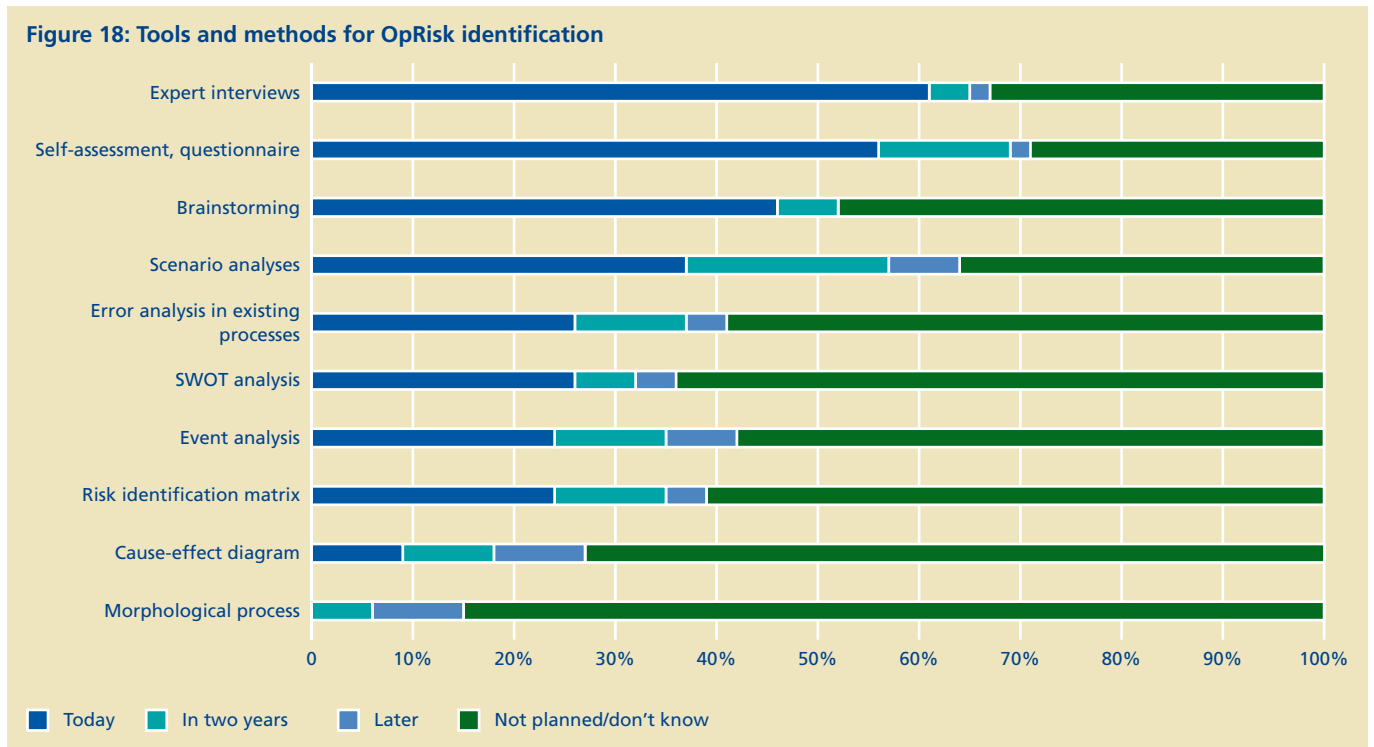
Today, 70% of the companies have already implemented risk monitoring or reporting and 65% OpRisk identification. Tools for internal communication have also been installed in the majority of cases. Insurers seem to have recognized that, in the risk management process too, there is the challenge of cultural integration into the actual company. On the contrary, external communication is not a primary focus for the moment. Risks are seldom measured or modelled systematically. Loss-data acquisition, an essential backbone for comprehensive ORM, is already rarely carried out systematically. Processes/systems for capital securitization are probably also still in the process of being set up in insurance companies for this reason (figure 17).<sup>5</sup>

Germany and Austria are generally further advanced than Switzerland with regard to implementation. In the next two years, more than 40% of the companies want to introduce solutions in the areas named. In this context company size does not play a significant role.

<sup>5</sup> The capital securitization of OpRisk is the ORM element with the second lowest degree of implementation (figure 17). On the other hand, the most recent studies point out that 13% of the average capital securitization requirement in the insurance industry concerns OpRisk. Thus, the 2007 Deloitte study "A stabilizing effect – the ICAS (Individual Capital Adequacy Standards) in action" mentions the following repartition of the average capital securitization requirement of insurance companies in Great Britain: insurance risk 41%, market risk 37%, OpRisk 13%, credit risk 8%, other 1%.

**Identification and assessment**

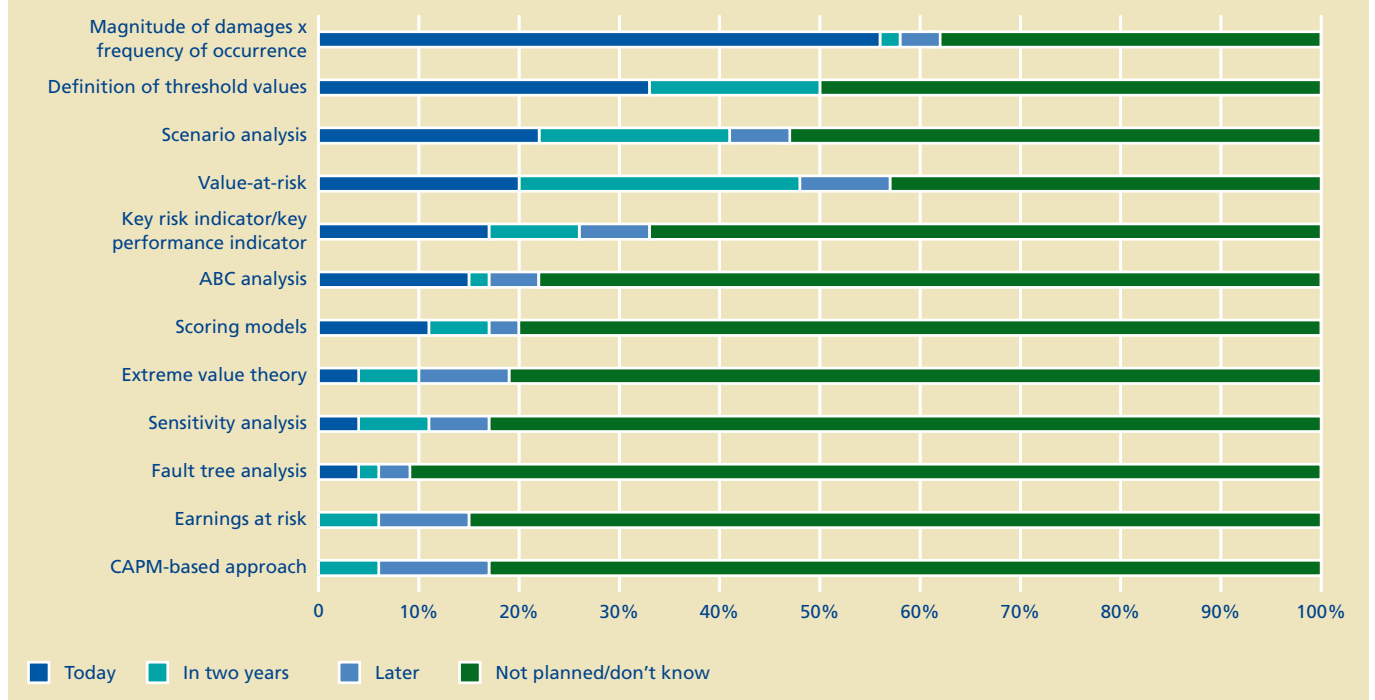
For identifying operational risks, more than half the surveyed companies primarily used expert interviews and self assessments (Figure 18). Brainstorming methods and scenario analysis were likewise frequently used. Large companies with high premium volumes today already use a larger number of tools and methods for OpRisk identification. In general, country-specific differences exist in this connection. In Switzerland, expert interviews were used less frequently, and self assessments or questionnaires more frequently, than in Germany and Austria.



For OpRisk assessment, various qualitative and quantitative tools and methods were called upon by the surveyed companies (figure 19). A significant majority of those questioned put their trust in a traditionally simple treatment of damage potential/probability. One third uses threshold values, while some 20% work with scenarios and the value-at-risk concept. On three of these four methods, the focus also lies on the company's preparatory work over the next two years. Advanced methods<sup>6</sup> are used by less than 10% of those questioned, whereas 80% of the companies are planning to work without such tools, even in the future. This could particularly be justified by the fact that the acquisition and modelling of risk data in the OpRisk area is made even more difficult as a result, and that the tool portfolio for OpRisk will be limited due to the heterogeneity and company-specific peculiarities of risk types.

<sup>6</sup> Like, for instance, scoring models, extreme value theory, sensitivity analysis, fault tree analysis, earnings-at-risk or capital market oriented approaches.

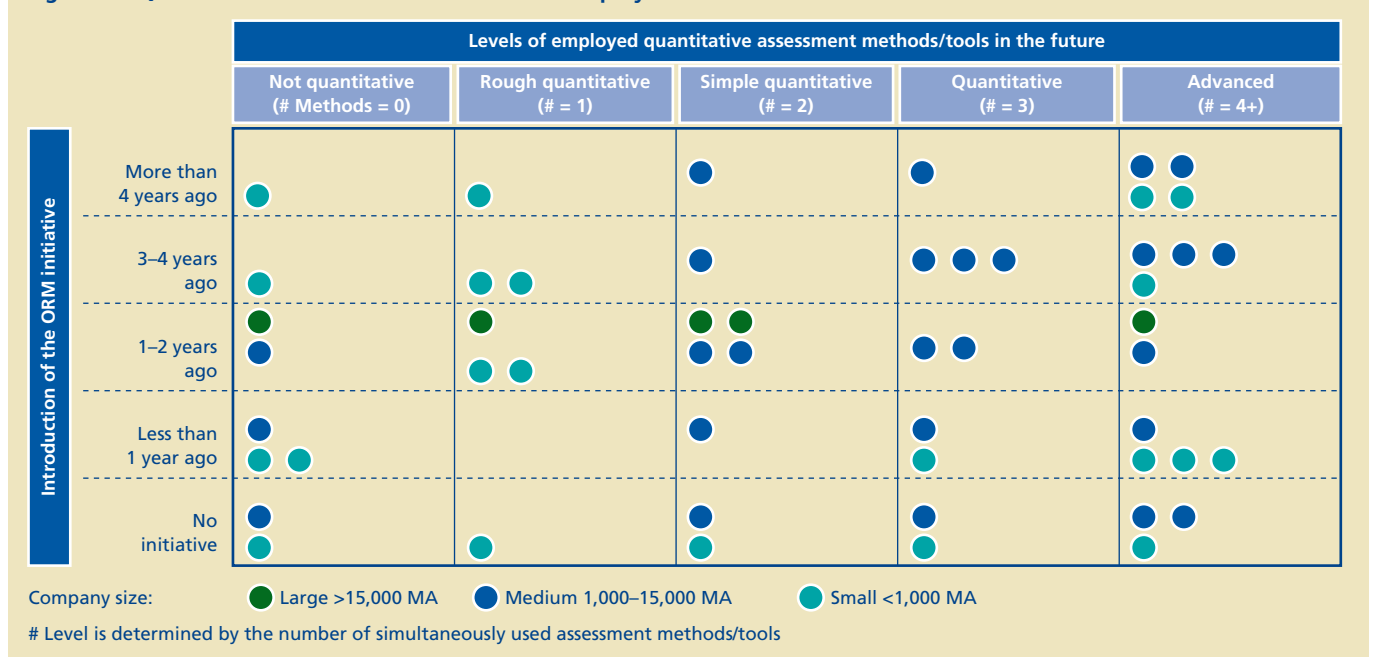
Figure 19: Tools and methods for OpRisk assessment



If the assessment methods/tools are pulled together with the timing of ORM initiation, it can be seen that today, medium-sized companies that introduced ORM three to four years ago, almost exclusively use advanced quantitative methods, i.e. a rich method set. The vast majority of companies, whose ORM program is more recent, use a distinctly simpler, smaller method set. This is more or less true for all large companies as well. The trade-off between data use and acquisition/calculation cost, and development over time is accentuated here.

If the planned use of methods and tools in the future is considered, it is shown that many companies in all size classes plan to organize their ORM a lot better quantitatively than they do today (figure 20). This is valid for all the categories considered, if the medium-sized companies that are already the most advanced – having started their ORM initiative 3 to 4 years ago – also intend to progress furthest in the future. In this connection, it is not unreasonable to speak of a really clear general trend towards higher quantification in ORM, independent of the initiation date of the ORM initiative. At the same time, the influence of increased regulation and the sector trend on integration into ERM is clearly shown.

Figure 20: Quantitative assessment methods to be employed in the future

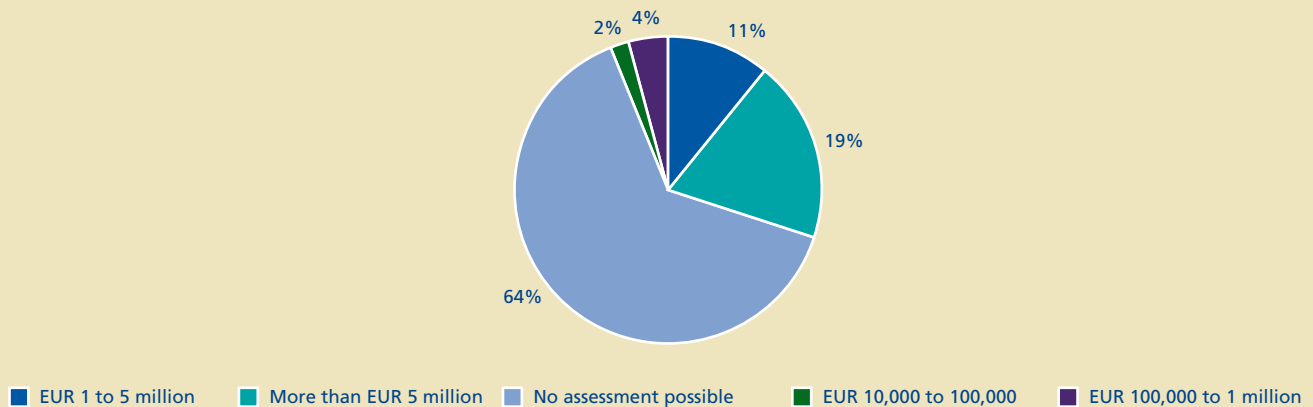


### Loss-data acquisition

On the one hand, the systematic acquisition of loss data is the ORM element with the lowest degree of implementation (figure 17) and on the other, useful data acquisition is a key prerequisite for determining damage potential in companies, i.e. risk identification, assessment and calculation.

If the results of the survey for the practical assessment of damage potential are considered, a clear picture emerges. At 64%, the majority of insurance companies questioned indicated that they were unable to assess the level of their annual OpRisk damages. 20% of the companies (figure 21) said that they could estimate the potential annual damage only approximately. Those companies that could make an estimate mostly mention amounts above five million Euros.

Figure 21: Annual damage potential from OpRisk



### Excursus: Risk-data acquisition

Risk-data acquisition can generally be made top down or bottom up, with considerable differences in meaningfulness and collection effort<sup>7</sup>. Moreover, the unavailability of forward-looking data, survivor bias<sup>8</sup> and the complexity of assessing risks with a low probability of occurrence, but a high degree of potential damage, are fundamental problems. For operational risks, the heterogeneity of risks, which can be distributed over all processes and areas of the organization and most of which are financially quantifiable only with difficulty, also arises. In particular, the following issues emerge:

#### 1. What is an event and how should it be recorded? Should all OpRisk events be recorded or only from a certain threshold?

- What threshold (i.e. lower limit) is appropriate, depends on the size and complexity of the company, but also on its respective risk policy. But how should near-event without damage consequences or events with a non-intended positive outcome be handled? In both cases, the (potential) damage amount can be covered, which increases the number of events, but also worsens the validity of the data.
- A further point is the question of how events should be recorded in a database. If the Basel II framework is used, entry according to the risk actuator depending on the definition and classification is appropriate. This assignment of individual risks was chosen by 65% of those surveyed. Classification would, however, be relatively rough. However, in order to understand the specific character of a risk event, from which concrete measures may also be derived, this must also be entered after the risk event has passed and after the risk repercussions<sup>9</sup>.

#### 2. Where and by whom should events be recorded?

Ideally, a reporting system, such as an internal control system for recording events exists, where the person responsible for risks can enter the corresponding data. In practice, this requires corresponding systems and employee knowledge. Without training and continuous support by system administrators or a central ORM, such a system cannot properly function. A further hurdle can be missing incentive structures for reporting events at all.

External databases or data exchange within a group represent one possibility for completing own data. In the insurance sector, professional offers already exist. None of the surveyed companies uses external data. Meaningful data exchange is thought to be difficult because of varying collection criteria and differences in company size, complexity and process structures. In addition, only a few insurance companies have appropriate databases. It is probable that this topic will increasingly become a focal point for establishing standards and progressively developing proposals for data sharing.

<sup>7</sup> Here, holistic acquisition, cause transparency and correlation between risks (advantage of bottom up) face collection effort and reaction speed.

<sup>8</sup> This means that statistically over time, only those units that have "survived" until today will be taken into consideration. The characteristic features of unsuccessful units are thus not considered in the analysis.

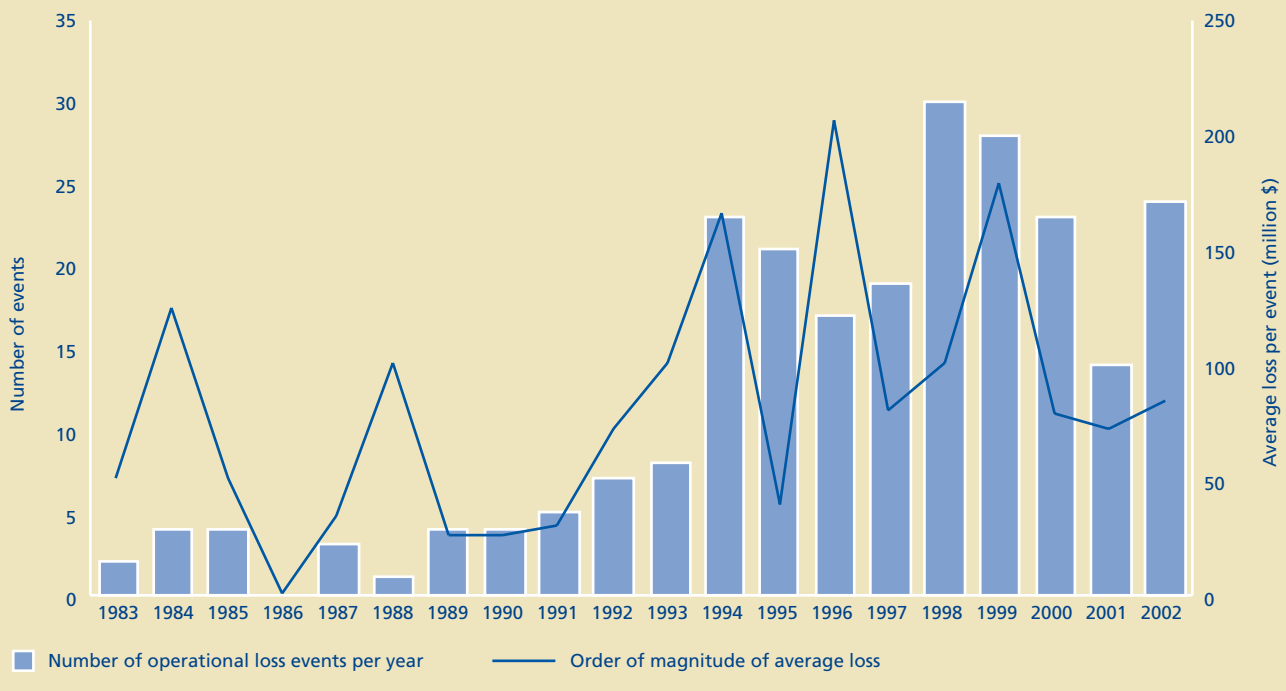
<sup>9</sup> Compare also with definitions and consideration levels of OpRisk in chapter 3.

**Excursus: Operational risk losses at US insurance companies**

The study "The Market Value Impact of Operational Risk Events for U.S. Banks and Insurers" analyzed operational events (i.e. losses based on operational problems) in insurance companies in the USA. In it, only losses of at least US\$ 10 million were analyzed.

It emerged that the average OpRisk loss for insurance companies (obtained from 241 events) was \$ 99.8 million (median: \$ 33.6 million). It is apparent that, over time, operational losses occur in closer and closer time intervals, and are thus linked with increasingly large absolute damage extents (figure 22).

**Figure 22: Frequency and order of magnitude of operational losses in the insurance industry**



Source: Cummins, J. David, Lewis, Christopher M. and Wei, Ran, "The Market Value Impact of Operational Risk Events for U.S. Banks and Insurers" (December 23/2004)

**Intermediate conclusion**

- The majority of the surveyed companies consider classic sub-processes in the risk-management process (communication, reporting) as being implemented.
- Loss-data acquisition, an essential basis for comprehensive ORM, rarely takes place systematically, which also explains the still low extent of modelling and capital securitization.
- Operational risks are today mainly identified and assessed by means of qualitative and simple quantitative methods. A clear trend to sophisticated methods is apparent in medium-sized companies with increasingly longer ORM initiative running times and in all the companies surveyed for the future.



# 5. Reporting

In order to define an individualized, optimally designed reporting system for each company, the main question is what general objective should be achieved by the overall company ORM. This originates from the risk policy (cf. chapter 2), in which the corporate ORM guidelines are formulated. Only based on the defined objective is it possible to address further important questions concerning the organization of a reporting system, and these are then tackled in a targeted way to achieve the individual objective.

Who is responsible for the reporting and what reporting lines should be considered? What form, content and scope should the reporting system have? At what moment should which addressee be informed? How were measures developed from the reporting results?

Within the framework of the study, focus was especially put on the form of reporting, internal as well as external, the reporting frequency and information recipients.

## Form of reporting (internal)

Internal reporting can consist of a daily status report of all OpRisk to management, be limited to reporting only events exceeding a certain threshold or reduced to simple loss-data acquisition with half-yearly reporting.

Differences in the form and specificity of the reporting are also shown in the study. Here, the following trends can be recognized:

- Almost all those surveyed have internal OpRisk reporting, with only 2% of insurance companies declaring that they did not carry out any internal reporting.
- In half of the insurance companies, internal reporting is part of the internal controlling system, and OpRisk categories are recorded and controlled separately (cf. chapter 3).
- 11% of the insurance companies, mainly the larger insurers with high premium volumes, declared they had a separate OpRisk report.

Independent of the chosen form of reporting, attention should basically be paid to ensure that all levels of the insurance company management are suitably supported by the reporting system, both contextually and procedurally, and that they are provided with adequate information.

## Form of reporting (external)

Within the legal framework requirements, supervisory authorities have been working for some years on the Solvency II project (EU) and the Swiss Solvency Test (Switzerland). Analogous to the three pillars in Basel II for banks, these guidelines describe three principles that solvency supervision will follow in future:

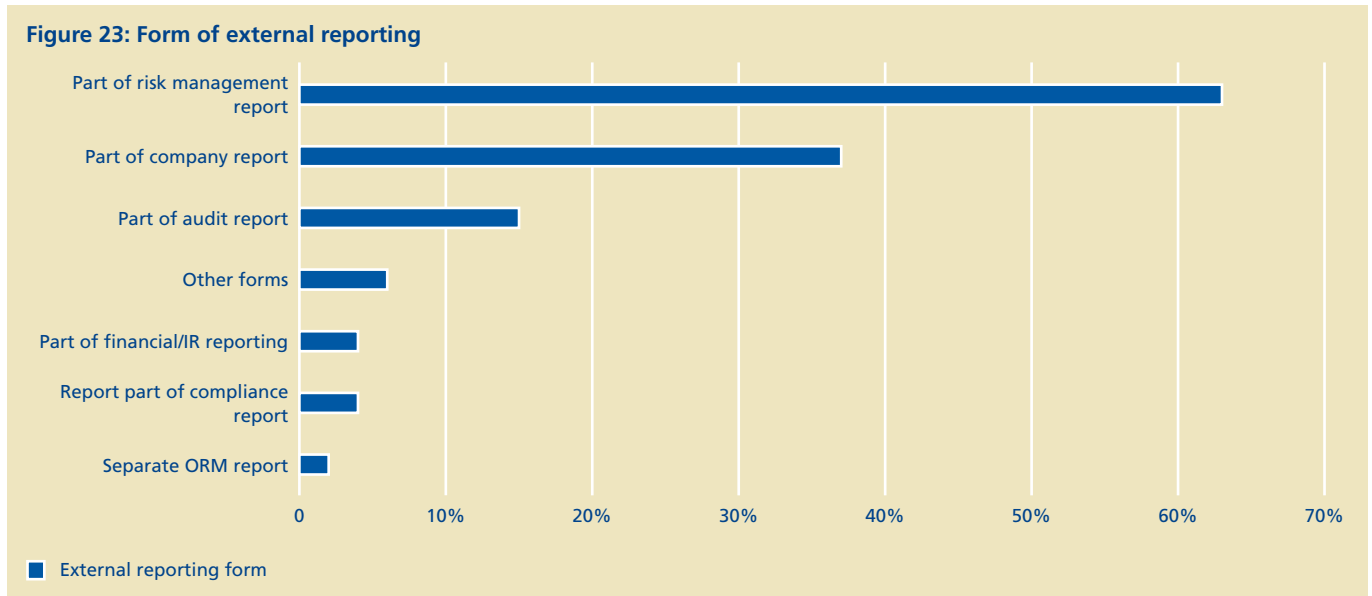
1st principle: Minimum demands on capital set-up

2nd principle: Auditing process according to supervisory regulations

3rd principle: Transparency

For external reporting, the 3rd principle in particular will be crucial in the future. It essentially concerns using existing market forces as a corrective, which is primarily reflected in extensive obligations to publish and strong dovetailing with the IFRS (International Financial Reporting Standards). At present however, Solvency II and the Swiss Solvency Test (SST) merely form a set of rules intended as a recommendation for insurance companies. But what is today's situation with regard to external OpRisk reporting in the German-speaking insurance sector?

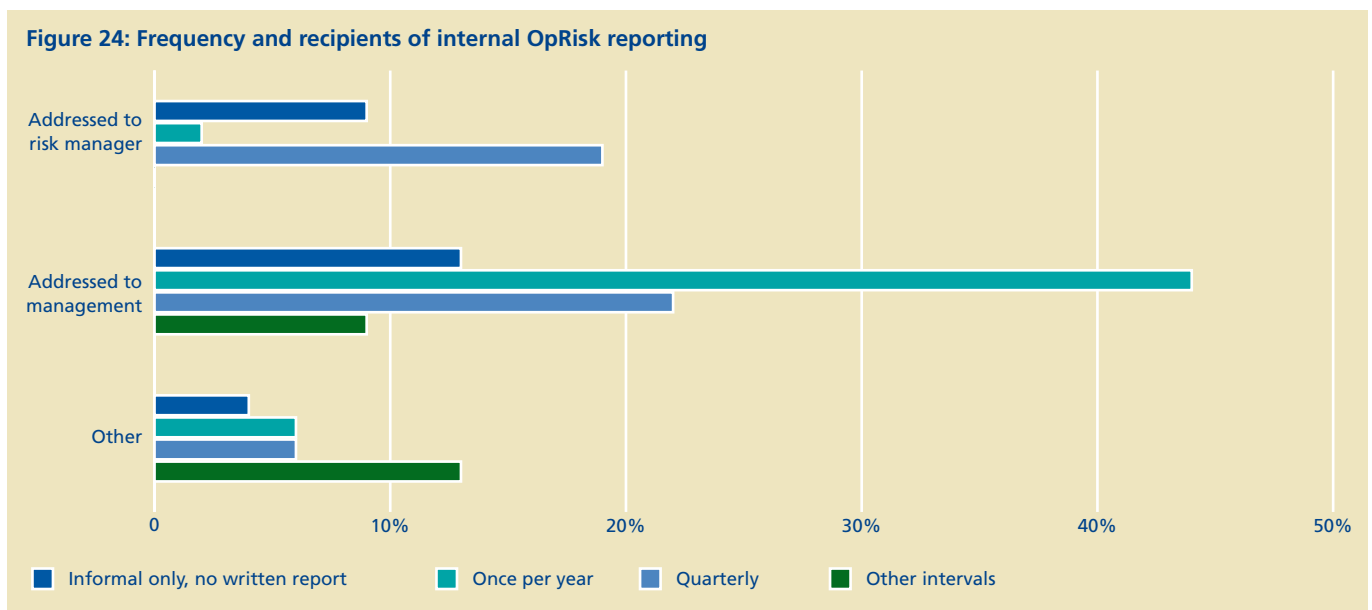
Analogous to internal reporting, the defined general objective of ORM is also crucial for the form of external reporting. Thus, the scope of reporting ranges from mentioning the topic of OpRisk as a part of risk management to descriptions of the ORM organization and the most important company-specific OpRisk in a special ORM report. The study makes it clear that, in contrast to internal reporting, external reporting is less widespread. For almost two thirds of the insurance companies that carry out external reporting, OpRisk reporting is part of the general risk-management report (figure 26). In addition, the presentation of OpRisk as part of the company report (37%) or of the audit report (15%) is widespread.



Based on a detailed evaluation, country-specific differences can be recognized. In Switzerland, OpRisk is only a minor topic of discussion both in the risk management report (33%) and in the company report (27%), whereas audit and compliance reports are more important. In particular, the larger companies (measured both by employee numbers as well as by premium volumes), mainly communicate by means of audit reports. In Germany, there is an opposite trend, with 85% identifying ORM as part of the risk-management report and almost half as part of the company report. Other forms of reporting are not very widespread in Germany. Similar tendencies are apparent in Austria, where in addition, 13% of insurance companies identify OpRisk as part of the financial report.

**Reporting frequency and information recipients**

Based on the differing and general ORM objectives of insurance companies, both the reporting frequency and the recipients of information also vary (figure 24). The survey additionally shows a dependency on both dimensions, which infers the existence of level-adapted reporting.



Thus, annual reporting, which in 44% of the cases is addressed directly to management, constitutes the norm. This trend is particularly evident in Switzerland. In 6% of the insurance companies, the report is sent to other internal target groups, with the parent company or supervisory/auditing offices in particular being mentioned most frequently. Only 2% of those questioned declared that they reported on a yearly basis to the risk manager. In Germany, reports are submitted more frequently, mainly on a quarterly basis. In the case of quarterly reporting, management, with 22%, still represents the most important target group. The internal report in this frequency, is also increasingly addressed to the risk manager, with 19%. Both in Switzerland and in Germany, reports are primarily addressed to management. In Austria, no clear trend has been identified.

**Intermediate conclusion**

- Internal OpRisk reporting is carried out by all those questioned, for half of whom it is part of the internal controlling system.
- The principle recipient of internal reports is management, being predominantly informed annually, followed by the risk manager with predominantly a quarterly reporting frequency.
- External reporting is carried out by 85% of those surveyed and is part of the risk-management or company report in the majority of cases.

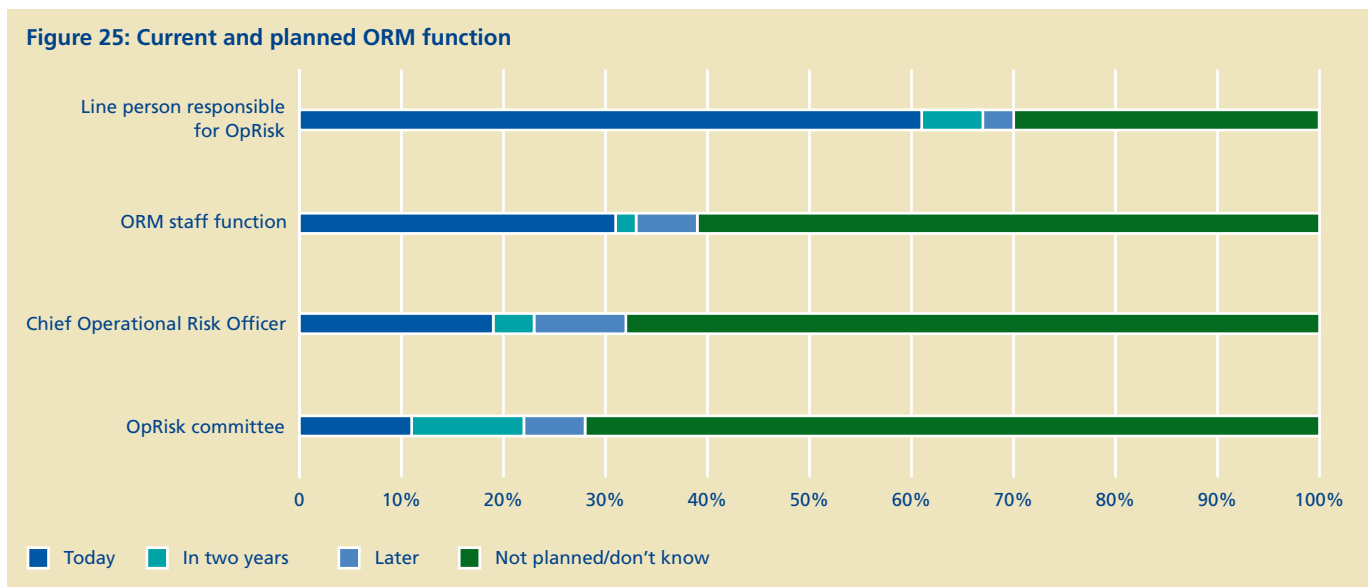
# 6. Risk governance and risk organization

Following explanations of the risk-management process and reporting with reference to the risk-management processes, this chapter deals with structural and organizational matters.

In the organization of risk governance, the following central questions arise: what does the ORM structure look like in German-speaking insurance companies? How many people work in ORM today and what is planned for the future? How is the current repartition of responsibility in the organization arranged? What other departments in the company are involved with ORM and form an interface to integral ERM? The answers to these questions give a first insight as to what importance is given to ORM in the company, and in particular by management. The tangible effects of this are shown in the structure of risk governance and risk organization, i.e. in the number of ORM jobs created and the assignment of responsibility, as well as in the other organization units involved in the ORM initiative.

## Structure of the risk organization

The study shows that a clear majority have at least one function in operational risk management. Thus, at the present time, 61% of the companies have a line manager who deals with ORM. For a further 10%, the introduction of such a function is planned (Figure 25).

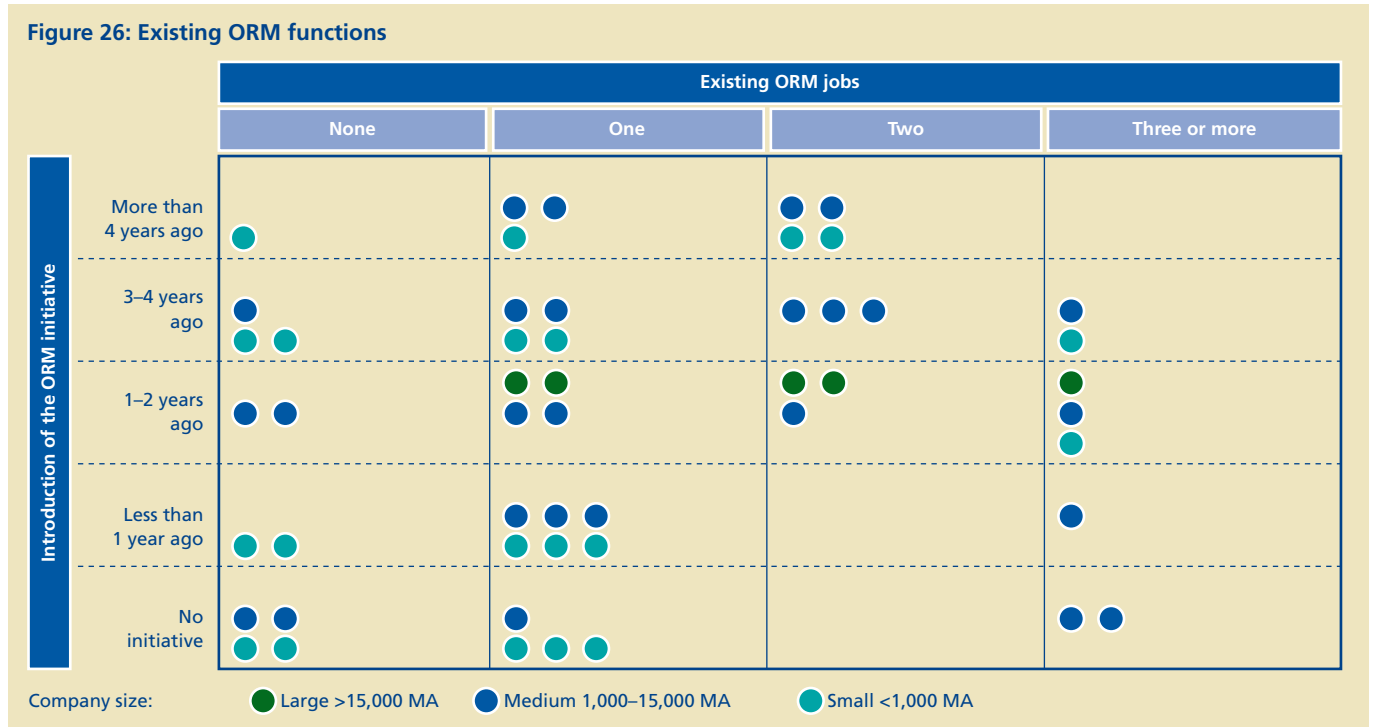


In the strictest sense, risk management is part of the ORM staff function. Almost a third of the companies surveyed had already institutionalized such a function, but however more than half of the companies have no plans for this. The situation with the chief operational risk officer looks similar. Only a fifth of the companies have a corresponding position and in nearly 70% of them, especially the smaller insurance companies, none is planned either. As a rule, the risk committee is responsible for risk policy at the management level, takes care that the management pays the necessary attention to ORM and thus represents the connecting link between the staff function and management. A specific OpRisk committee exists in only 11% of cases but is, however, being planned by 17% of the insurance companies surveyed. Furthermore, the study identified country-specific trends. In Switzerland, many ORM staff functions are already in existence. The larger multinational insurance companies, above all in Germany and Austria, have, however, frequently defined line personnel as responsible for OpRisk.

**Creation and development of governance structure**

The study shows a clear connection between the existence of an ORM function and the number of employees in the insurance company.

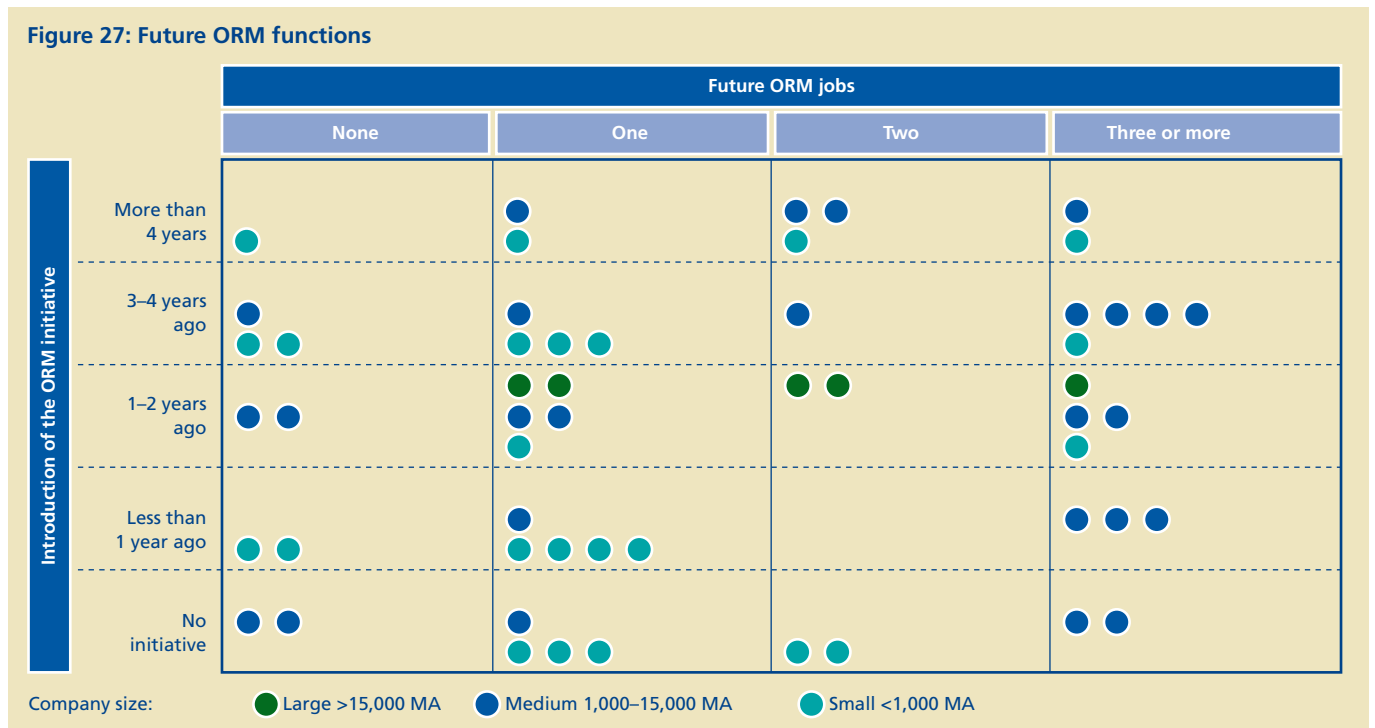
**Figure 26: Existing ORM functions**



The majority of insurance companies have introduced an ORM function, the smaller companies tend to have only one, while the medium and larger companies frequently have several. It is further apparent that, more frequently than the medium- and large-sized insurance companies, the smaller ones had only introduced such a function within the past year, or as yet, not at all (figure 26).

In future, the majority of those insurance companies that as yet have no ORM are planning to establish their own ORM functions. Only two insurance companies without an ORM initiative do not plan to create a corresponding position (figure 27).

**Figure 27: Future ORM functions**



## Management of Operational Risks in Insurance

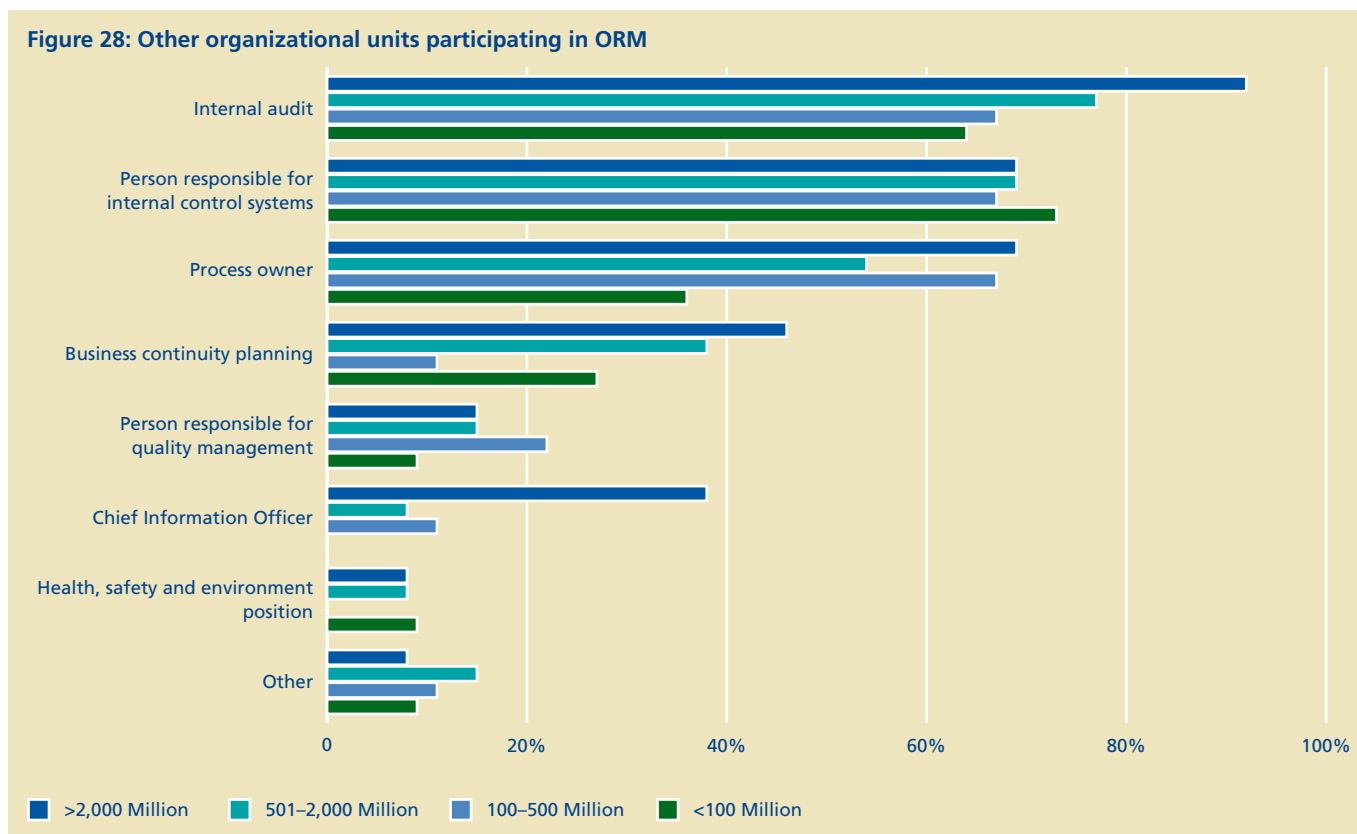
In companies that have had an ORM strategy for one to two years, no expansion plans with regard to the functions were identified. In contrast to this, insurance companies that have been following an ORM strategy for three to four years show the highest growth with regard to new functions. This development will lead to a deeper rift between the two groups of companies. Those insurance companies with very recent ORM initiatives (less than one year) are interested in extensively building up their ORM functions, but will have to make huge efforts in order to close the existing gaps. It is an interesting fact that medium-sized companies which have to date not yet implemented ORM, tend towards the introduction of either no positions at all or many of them in ORM. For their part, the smaller companies plan to create one to two positions in the future.

### Repartition of responsibility in risk organization

The institutionalized participation of management – management attention – is a decisive prerequisite for successfully tackling OpRisk. On the corporate management level, it is apparent from the study that, in practice, in 44% of the insurance companies surveyed, overall responsibility for ORM lies with management. In 20% of those questioned, the CEO was named. The CFO as the person with overall responsibility, with 6%, represents the exception case. A similar picture emerges with regard to the responsibility for developing risk policy and risk strategy. In view of its many facets, together with overall responsibility for ORM, great significance is also attached to the definition of roles, tasks and responsibilities of all the other ORM functions. As the study shows, the responsibility and task definitions for the functions subordinated to management are, however, hardly ever institutionalized. In the future, there will be a need for further action by insurance companies, and this will depend on the one hand on the company size and, on the other, on the degree of implementation of the ORM initiatives, and there will thus be corresponding variances between them.

### Departments involved and interfaces to ERM

Risk management touches on various areas of responsibility. Links between already existing systems and ORM initiative may also be seriously affected. This is reflected predominantly by the participation of the internal control system and internal auditing in ORM. In companies with high premium volumes (more than EUR 2 billion), other organizational units very often participate in ORM. In particular, the Chief Information Officer is regularly involved in ORM, which gives an indication as to what importance is basically given to technology risks (figure 28).



### Intermediate conclusion

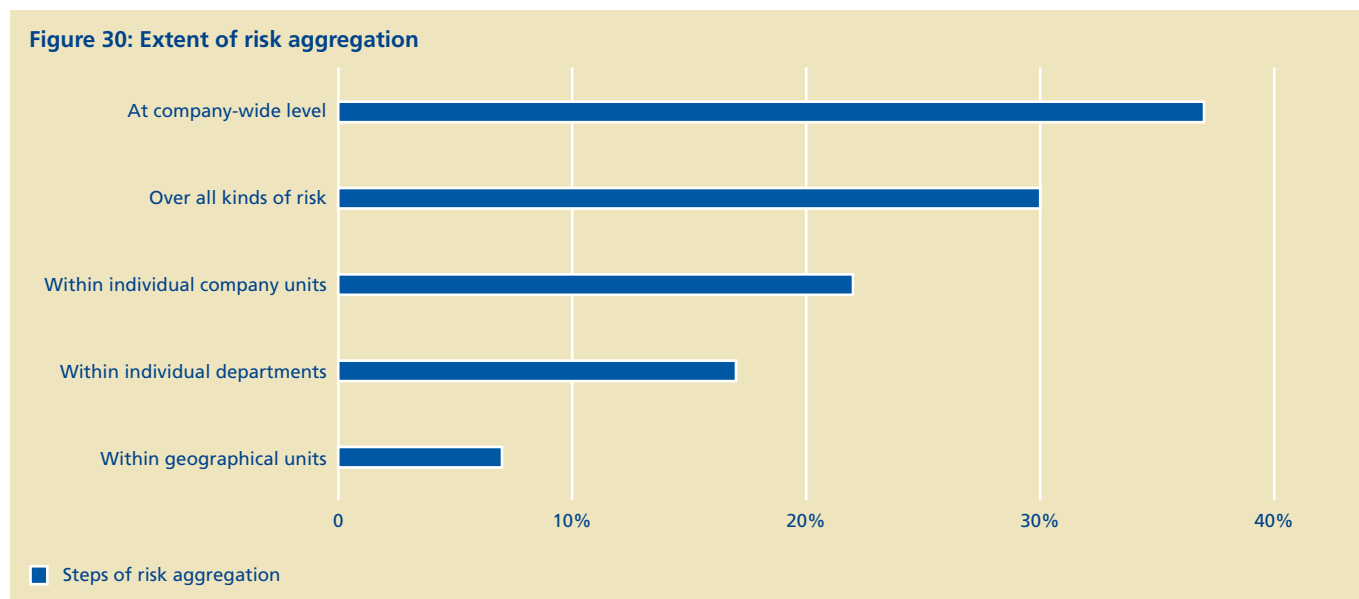
- The majority of companies surveyed have at least one ORM function (e.g. line person responsible for OpRisk).
- In two thirds of cases, overall responsibility is taken by management as a whole or by the CEO. However, other responsibilities such as loss-data acquisition are, in most cases, not yet institutionalized.
- The still inadequate institutionalization has to do with the fact that numerous other organizational units participate in ORM. This demands an organizational structure and the consideration of interfaces with the ORM function.

# 7. Integration of ORM into enterprise risk management (ERM)

The objective of enterprise risk management (ERM) is the integral examination of a company’s risk situation, which results in an optimized operational and interdisciplinary control of all risks in the company. For this reason, the management of operational risks also becomes a focus of consideration for ERM. Thus, both the company-inherent and the Solvency II/Swiss Solvency Test points of view are taken into consideration.



Although the survey shows that the desire for comprehensive ERM is one of the main driving factors for the development of ORM, procedural or resource gaps frequently exist in the concrete implementation of risk-management strategies. Procedural gaps are created due to missing or insufficient integration into ERM, while resource problems can be attributed to deficient or missing specialist qualifications. This problem is aggravated by the fact that current regulatory developments (Solvency II, SST) initially focus on financial security and that management sets a lower priority for the supervision of frequently unquantifiable OpRisk. Thus, 15% of the companies explicitly stated that ORM is not integrated into ERM. Two thirds have implemented integrated risk reporting and almost 60% work with integrated risk identification or risk prioritization. A country-specific comparison shows that integrated risk reporting is less widely distributed in Austria. While Austrian insurance companies plan no integrated risk modelling or risk measurement, in both Switzerland and Germany, a fifth of the companies surveyed make use of this high level of integration (figure 29).



If integration is planned, this is mostly at a company-wide level (37%). However, in 30% of the companies, all types of risk are aggregated together and in 22%, they are aggregated within the individual company units. It should be noted here that every fifth company gave no details concerning to what extent risk aggregation takes place. Insurance companies with low premium volumes seldom aggregate risks all together. This leads to the conclusion that the insurance companies surveyed place the emphasis for controlling operational risks at different decision levels (figure 30).

### Intermediate conclusion

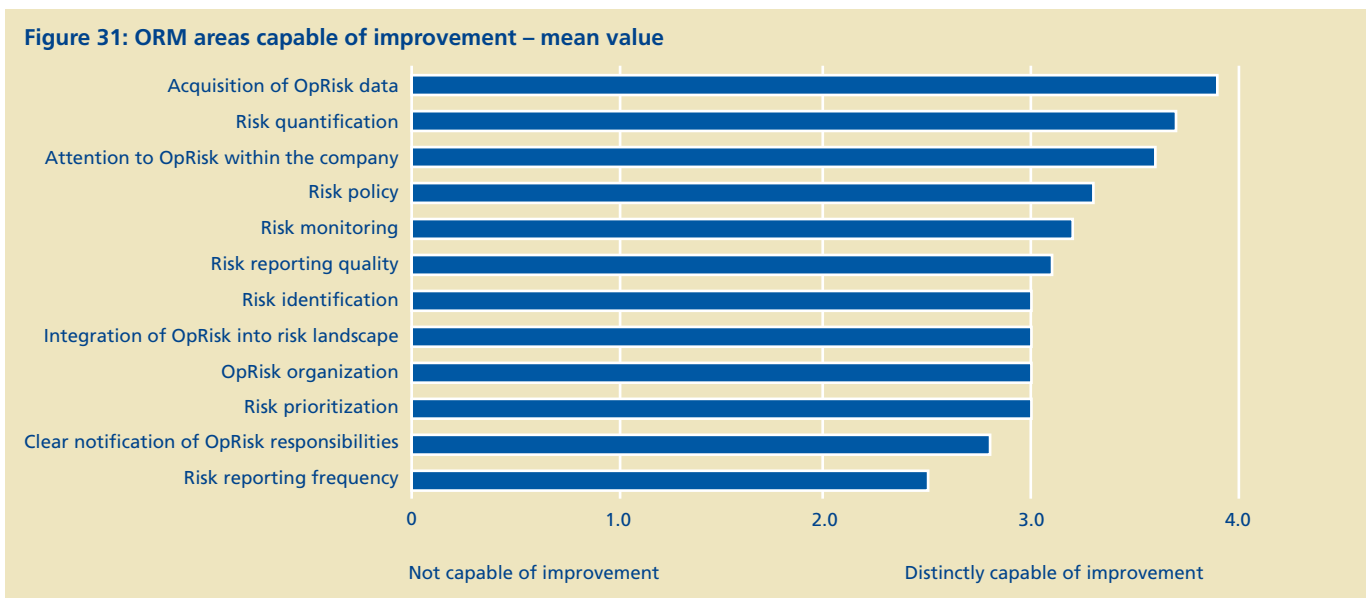
- ERM is one of the main driving factors for the development of ORM.
- In general, considerable effort is still necessary in order to accomplish the integration of ORM into ERM.
- There are large differences in risk aggregation with regard to the decision level. The company-wide level was the most frequently mentioned.



# 8. Way forward

The study shows that the insurance sector is today also orienting towards ORM as the target system, whether for reasons of regulatory pressure or strategic planning. What do the companies surveyed now see as the necessary steps for further development? Independently of the declared status of individual ORM initiative elements (cf. chapter 4), companies see a moderate to strong need for action in all areas (figure 31).

On the one hand, stated concerns about insufficient implementation have been confirmed in the case of acquisition of OpRisk data and the use of quantitative methods. On the other hand, it is clear that, even in the case of ORM elements considered as extensively introduced, such as, for example risk identification and monitoring, a need for improvement is perceived. Furthermore, as a process, ORM receives quite high attention from management, and OpRisk organizations have been and will be expanded (cf. chapter 6). The awareness of OpRisk in the overall organization, however, is clearly described as "needs to be improved". Something similar applies in the perception that risk policies have room for improvement, even if OpRisk is, in principle, seen as covered by general risk policies. It can therefore be concluded that companies consider this coverage to be insufficient.



**Intermediate conclusion**

- In all the areas considered, the need for action is perceived as moderate to high. The necessity for consistent ORM is increasingly coming to the fore.
- There is considerable need for action in the area of OpRisk data acquisition and risk quantification.
- Consideration is being given to improving the quality of already implemented ORM elements (e.g. risk monitoring).

# 9. Focus on Switzerland

ORM is relatively new in Switzerland. While 19% of insurance companies in Germany and 13% in Austria have been active in ORM for more than 4 years, this is the case for only one of the companies surveyed in Switzerland (figure 32). In most cases, the ORM initiatives were also initiated because of regulatory guidelines rather than for strategic considerations. For most insurance companies, the consequence of this is that ORM is frequently less developed than it is in German or Austrian companies. For those companies that are strongly oriented towards, and are faithful to, rules and regulations, it is important not to lose sight of the strategic components of ORM.

For this reason, in comparison to Germany and Austria, ORM in Swiss insurance companies has a number of particularities, which are briefly presented below.

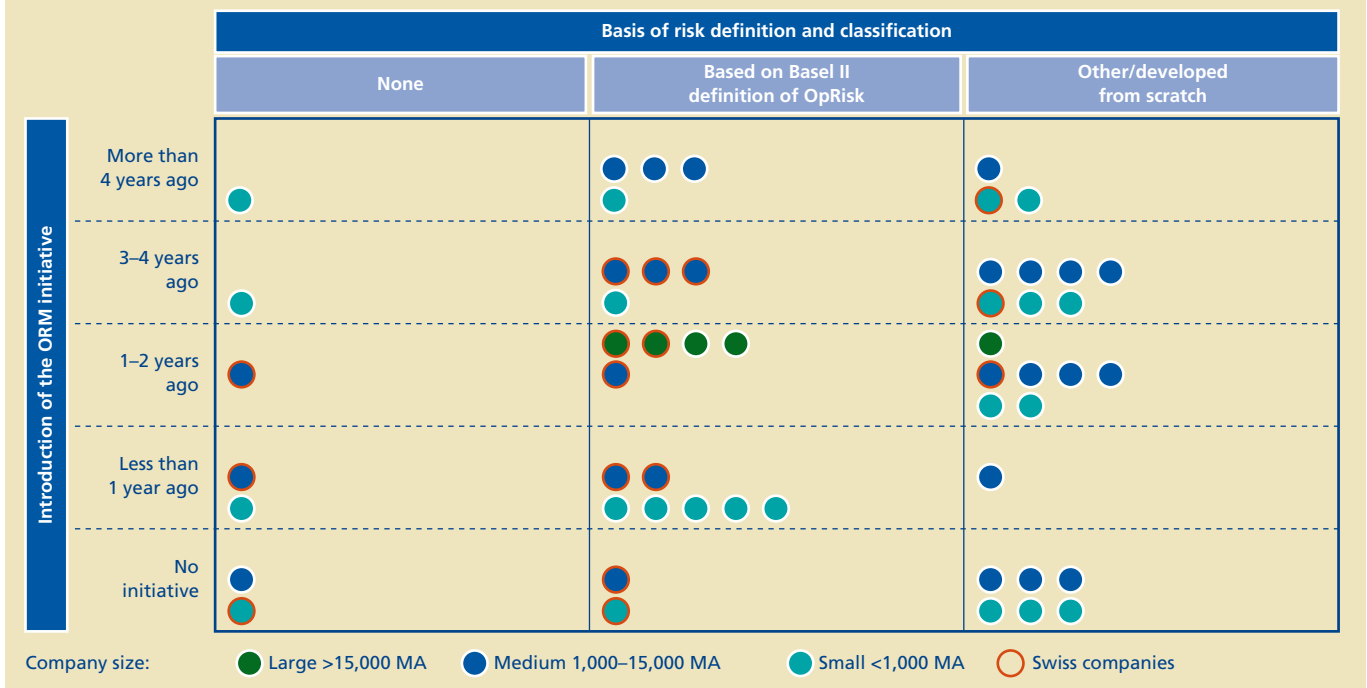
### Governance and organisation

In Switzerland, a relatively high number of insurance companies already have a specific OpRisk policy. This results from the major influence of regulatory guidelines. However, there is still potential for improvement in the area of organization. Thus, OpRisk is only rarely included as part of the internal control system. In order to benefit from synergies, it would make sense to link ORM with the internal controlling system, with which it already overlaps in certain areas.

### Risk definition/classification

In Switzerland, insurance companies mostly follow the risk definitions and classification according to Basel II, and the majority use Basel II as a general basis (figure 32). "Inadequately defined processes" were cited as the most important operational risk in Switzerland, whereas IT security gaps and system interruptions were rated much lower than in Germany or Austria.

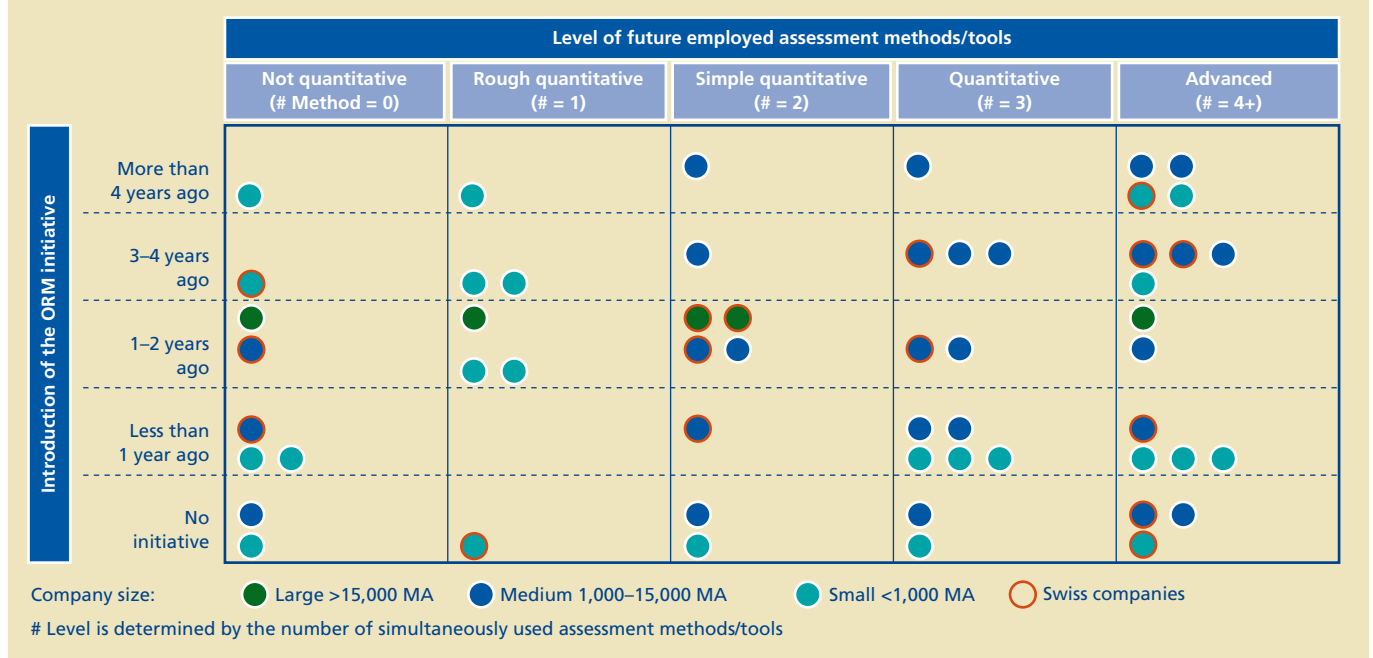
Figure 32: Basis of risk definition and classification in Switzerland.



**Risk management process**

Swiss insurance companies are frequently less successful in assessing damage potential. They generally calculate with higher losses than their foreign competitors. In Switzerland the coverage of OpRisk is often carried out on a high level. A few companies also record and administer them separately (figure 33).

**Figure 33: Quantitative assessment methods/tools to be employed in the future in Switzerland**



**Reporting**

In comparison with the other countries, external reporting in Switzerland is more often carried out within the framework of the auditing report and less frequently in the risk-management or company report. In addition, OpRisk in Switzerland is sometimes listed in the compliance report or in a special ORM report.

**Implementation**

Swiss insurance companies basically lag behind in the implementation of almost all elements of OpRisk. Thus, for instance, risk monitoring and reporting, as well as external risk communication, have been implemented by only some half as many companies in Switzerland.

**Outlook**

Swiss insurance companies want to shape the development of qualitative and quantitative methods. In the future, they would prefer to go in the direction of advanced quantitative assessment methods. It is clear that the existing potential for improvement has been recognized. If the Swiss companies succeed in implementing their future plans as desired, they must at least keep pace with existing quantitative standards and in many cases even be able to set them.

**Intermediate conclusion**

- ORM is a relatively young process in Switzerland, the primary driving factor for its initiation being regulatory guidelines.
- Consequently, a few particularities have developed in the Swiss insurance sector, such as the above-average orientation towards Basel II, in particular when designing the ORM initiative.
- In the implementation of ORM, Swiss insurance companies lag slightly behind those in Germany and Austria, but they have already recognized that potential for improvement exists in the future.

## 10. Conclusions and outlook

ORM is increasingly becoming the focus of attention in the insurance sector. Because of regulatory developments (Solvency II, SST), all companies will be basically obliged to establish an appropriate risk-management system. From the present study, it is evident that those companies that began implementation because of internal strategic considerations have more widely developed tools and methods at their disposal, and are already benefiting from the advantages that can be achieved by effective ORM, such as improved process quality, better risk prevention and enhanced emergency planning.

However, for the whole sector, while there is definitely sensitivity with regard to OpRisk, ORM is still in the development phase, and companies are confronted with various issues because of the idiosyncrasies of this risk category.

### Driving factors

The main reasons for introducing ORM are regulatory pressure, the need for a comprehensive risk overview and protection from OpRisk related losses. It is evident that companies with older ORM initiatives increasingly emphasize strategic reasons for the introduction of ORM, while companies with younger processes are driven by regulations. The importance of strategic ORM initiatives is recognized by the insurance companies, but this may be attributed to a high degree of attention by management: most of the processes were started by management/the CEO.

### OpRisk policy and strategy

Most of the insurance companies surveyed have a risk policy that also covers OpRisk, whereas a mere 10% of them, mainly the large companies, have also implemented a specific OpRisk policy for OpRisk. Over a quarter of the smaller companies have still not implemented any policy, so for these, there is a more pressing need for action. However, only a third of the companies that do have a policy have also turned this into basic strategies for managing OpRisk.

### Risk identification and classification

Basel II is also used by a large percentage of insurance companies for orientation with regard to the definition and classification of OpRisk. Multi-stage, complete classification according to the costs-by-cause principle (cause, event, loss) is still rarely applied by insurance companies. Operational risks are assessed differently in different countries, with legal and political risks, IT risks, inadequately defined processes and the turnover of key personnel generally being assessed as critical. The growing relevance of ORM in the insurance sector will in the future also lead to OpRisk definition and classification being increasingly adapted to the specific needs of insurance companies.

### Risk management process

The majority of the companies surveyed consider classic sub-processes in the risk-management process (communication, reporting) as being implemented. Loss-data acquisition, an essential basis for complete ORM, rarely takes place systematically, which also explains why the extent of modelling and capital securitization is still limited. Today, risks are predominantly identified and assessed by means of qualitative and simple quantitative methods (e.g. self-assessment). A clear trend to sophisticated methods, which increases with the maturity of the ORM initiative, is apparent in medium-sized companies today, as well as in all the companies surveyed in the future.

### Reporting

Internal OpRisk reporting is carried out by all the companies surveyed. For half of them it is part of the internal controlling system. The principle addressees of internal reports are management, which for the most part is informed annually, followed by the risk manager, where the reporting frequency is predominantly quarterly. External reporting is carried out by 85% of the companies surveyed, and is, in the majority of cases, part of the risk-management or company report.

### Risk governance and risk organization

The majority of companies surveyed have at least one ORM function (e.g. line person responsible for OpRisk). In two thirds of cases, overall responsibility is taken by management as a whole or by the CEO. Other responsibilities, such as, for instance, loss-data acquisition are, however, in most cases not yet institutionalized. The still inadequate institutionalization has to do with the fact that numerous other organizational units participate in ORM. This demands for a clear organizational structure and consideration of its interfaces with the ORM function.

## ORM and ERM

ERM is one of the main driving factors for the development of ORM. There are considerable gaps in the implementation of integration. There are large differences in risk aggregation with regard to the decision level. The company-wide level was the most frequently mentioned.

## Way forward

In all the areas considered, the need for action is generally perceived as moderate to high. The necessity of a consistent ORM is also increasingly understood. There is considerable need for action in the area of OpRisk data acquisition and risk quantification. Further, consideration is being given to improving the quality of already implemented ORM elements (e.g. risk monitoring).

## Focus on Switzerland

ORM is a relatively young process in Switzerland, the primary driving factor for its initiation being regulatory guidelines. Consequently, a few particularities have developed in the Swiss insurance sector, such as the above average orientation towards Basel II, in particular when designing the ORM initiative. In implementation, the Swiss insurance companies lag behind, although they have recognized existing potential for improvement in the future.

### Excursus: Special focus and trend groups

#### Small companies: facing considerable challenges

Small companies are not in the lead in any ORM area. This lagging behind stems from the fact that these companies only began elaborating ORM recently and have few specialists and little financial resources for risk management. The smaller insurance companies almost exclusively started working on an ORM strategy for regulatory reasons. None of these companies is in a position to assess the annual OpRisk damage potential concerned. This is not really astonishing, since practically no quantitative assessment methods and only few qualitative approaches have been established in these companies. These gaps have been recognized by most small companies and, in the methods area, should be closed by further expanding ORM. In part, they are also planning a huge expansion of ORM jobs and functions. While today, there is not more than one employee per company, in future, on average, three people are planned in the ORM area.

#### Big companies: only slow progress

In the largest companies (more than 15,000 employees), there is a very inconsistent picture in the various application areas. The large companies have strongly oriented the organization of their ORM framework towards Basel II. That there is no tendency in the large companies to strive for improvements is serious, although various gaps have been clearly identified. Here too, for the moment, qualitative methods, particularly for identification, are primarily used. The use of quantitative methods is not planned. Likewise, there is a tendency to renounce building up ORM jobs and functions (today 100 to 200 full-time jobs).

#### Medium-sized companies: leaders of the pack

Medium-sized companies have the most advanced approaches in practically all areas. In addition, in contrast to the big companies, they show interest in the further development, or rather the continual improvement and extension, of their ORM initiatives. As opposed to the small insurance companies, the decision to develop ORM is not driven exclusively by regulation tendencies. Strategic considerations play a decisive role. This proactive approach may also be the reason for the identifiable progress. Consequently, it is the medium-sized companies which succeed best in assessing their annual damage potential. Similarly, they tend to plan to build up ORM functions and jobs in the coming years. With the methodical implementation of this plan, the most comprehensive approaches should be found in the medium-sized companies.

# Authors and contacts

## Deloitte

Dr. Daniel Kobler  
Strategy & Risk Consulting  
Tel: +41 (0)44 421 68 49  
dkobler@deloitte.ch

Sandro Schmid  
Head of Risk & Performance Management  
Tel: +41 (0)44 421 62 48  
sschmid@deloitte.ch

Sabine Betz  
Actuarial & Insurance Solutions  
Tel: +41 (0)44 421 68 81  
sbetz@deloitte.ch

Bharat Bhayani  
B&W Deloitte GmbH  
Tel: +49 (0)221 973 24 13  
bbhayani@bw-deloitte.de

## Institute of Insurance Economics of the University of St. Gallen

Dr. Bernard El Hage  
Area Manager, Trend Monitoring  
Tel: +41 (0)71 243 40 61  
bernard.elhage@unisg.ch

Matthias Heer  
Project Leader, Risk Management  
Tel: +41 (0)31 325 84 79  
matthias.heer@unisg.ch



In this publication, Deloitte refers to one or more of Deloitte Touche Tohmatsu ('DTT'), a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. As a Swiss Verein (association), neither DTT nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte", "Deloitte & Touche", "Deloitte Touche Tohmatsu", or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the DTT Verein.

In the UK, Deloitte & Touche LLP is the member firm of DTT, and services are provided by Deloitte & Touche LLP and its subsidiaries. For more information, please visit the firm's website at [www.deloitte.co.uk](http://www.deloitte.co.uk)

Deloitte & Touche LLP is authorised and regulated by the Financial Services Authority.

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication.

Deloitte & Touche LLP would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte & Touche LLP accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication

© Deloitte & Touche LLP 2007. All rights reserved.

Deloitte & Touche LLP is a limited liability partnership registered in England and Wales with registered number OC303675. A list of members' names is available for inspection at Stonecutter Court, 1 Stonecutter Street, London EC4A 4TR, United Kingdom, the firm's principal place of business and registered office.  
Tel: +44 (0) 20 7936 3000. Fax: +44 (0) 20 7583 1198.

Designed and produced by The Creative Studio at Deloitte, London.

Member of  
**Deloitte Touche Tohmatsu**