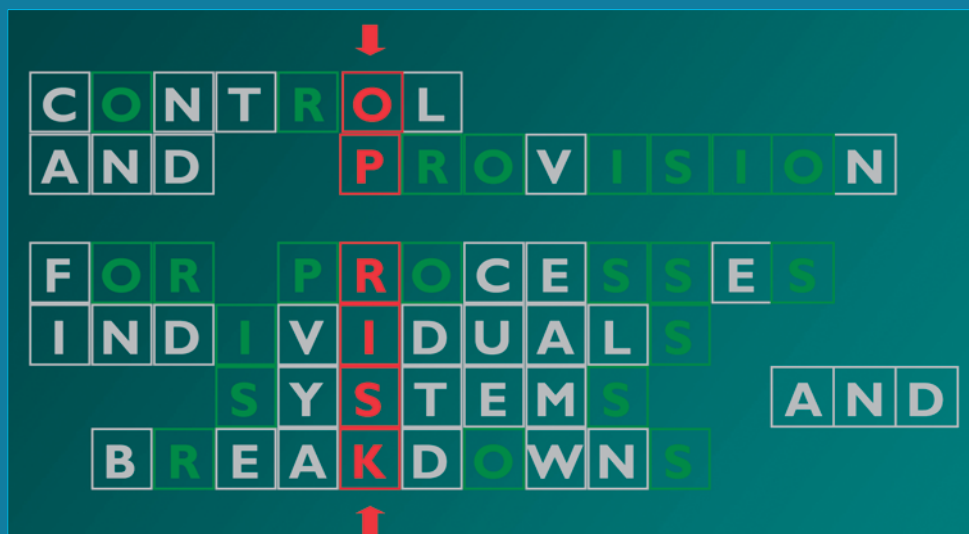


# GUIDELINES ON **Operational Risk Management**



*These guidelines were prepared by the Oesterreichische Nationalbank  
in cooperation with the Financial Market Authority*

**Published by:**

*Oesterreichische Nationalbank (OeNB)*  
*Otto-Wagner-Platz 3, 1090 Vienna, Austria*  
*Austrian Financial Market Authority (FMA)*  
*Praterstraße 23, 1020 Vienna, Austria*

**Produced by:**

*Oesterreichische Nationalbank*

**Editor in chief:**

*Günther Thonabauer, Communications Division (OeNB)*  
*Barbara Nösslinger, Staff Department for Executive Board Affairs and Public Relations (FMA)*

**Editorial processings:**

*Chapter I and III: Roman Buchelt, Stefan Unteregger (OeNB)*  
*Chapter II and IV: Wolfgang Fend, Radoslaw Zwizlo, Johannes Lutz (FMA)*

**Design:**

*Peter Buchegger, Communications Division (OeNB)*

**Typesetting, printing and production:**

*OeNB Printing Office*

**Published and printed at:**

*Otto-Wagner-Platz 3, 1090 Vienna, Austria*

**Inquiries:**

*Oesterreichische Nationalbank*  
*Communications Division*  
*Otto-Wagner-Platz 3, 1090 Vienna, Austria*  
*Postal address: Post Office Box 61, 1011 Vienna, Austria*  
*Phone (+43-1) 40420-6666*  
*Telefax (+43-1) 40420-6696*  
*Austrian Financial Market Authority (FMA)*  
*Executive Board Affairs & Public Relations Division*  
*Praterstraße 23, 1020 Vienna, Austria*  
*Phone (+43-1) 24959-5100*

**Orders:**

*Oesterreichische Nationalbank*  
*Documentation Management and Communications Services*  
*Otto-Wagner-Platz 3, 1090 Vienna, Austria*  
*Postal address: Post Office Box 61, 1011 Vienna, Austria*  
*Phone (+43-1) 40420-2345*  
*Telefax (+43-1) 40420-2398*

**Internet:**

*<http://www.oenb.at>*  
*<http://www.fma.gv.at>*

**Paper:**

*Salzer Demeter, 100% woodpulp paper, bleached without chlorine, acid-free, without optical whiteners*

**DVR 0031577**

# Preface

Given the rising complexity of banking, which results from internationalization, expansion and change in business activities, the increasing use of innovative financial products (securitized products, credit derivatives, structured products) and the significance of modern information technologies, the new regulatory capital framework (Basel II) also includes requirements for risk management as well as a regulatory capital charge for “operational risk”.

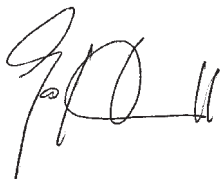
In part, this risk category has already been studied in internal risk analyses. Depending on the size and complexity of a bank, the response to operational risks may require considerable changes, such as the adaptation of systems and processes as well as, above all, the further development and integration of risk management methods.

The present guidelines on **“Operational Risk Management”** are to support banks in designing and adapting the systems and processes required when they implement Basel II. The issues presented are in line with international developments in banking that focus on a comprehensive approach to, and the optimum handling of, operational risks so that their implementation would make sense even in the absence of new capital requirements.

The purpose of these guidelines is to develop a common understanding shared by supervisory authorities and banks with regard to the forthcoming changes in banking. In this context, the Oesterreichische Nationalbank (OeNB) and the Financial Market Authority (FMA) see themselves as partners to Austria’s credit industry.

It is our sincere hope that these guidelines provide interesting reading as well as a basis for the efficient discussion of current changes in the Austrian banking sector.

Vienna, August 2006



Josef Christl  
Member of the Governing Board  
of the Oesterreichische Nationalbank


Kurt Pribil,  
Heinrich Traumüller  
FMA Executive Board

# Contents

<b>1 Causes and Definition of Operational Risk</b>	<b>7</b>
1.1 Introduction	7
1.2 Definition of Operational Risk	8
1.3 Characteristics and Importance of Operational Risk	10
1.4 Case Studies	15
<b>2 Methods of Operational Risk Management</b>	<b>18</b>
2.1 Introduction	18
2.2 Organizational Framework Conditions	19
2.2.1 Framework	19
2.2.2 Roles and Responsibilities	19
2.3 Step-by-Step Introduction of Operational Risk Management	21
2.3.1 Starting Point	21
2.3.2 Raising Awareness and Creating the Basis	22
2.3.3 Implementation	22
2.3.4 Enhancements and Ongoing Adaptation	22
2.3.5 Integration into Bank-Wide Capital Allocation and Risk Management	23
2.4 Operational Risk Management as a Cycle	23
2.5 Risk Identification and Assessment	24
2.5.1 Self-Assessment (Risk Inventory)	25
2.5.2 Loss Database	27
2.5.3 Business Process Analysis	29
2.5.4 Scenario Analysis	30
2.5.5 Key Risk Indicators (KRIs)	32
2.5.6 Quantification of Operational Risk	33
2.5.7 Exemplary Approaches to Calculating Regulatory Capital	36
2.6 Risk Treatment	37
2.6.1 Risk Avoidance	38
2.6.2 Risk Mitigation	38
2.6.3 Risk Sharing and Transfer	38
2.6.4 Risk Acceptance	43
2.7 Risk Control	43
2.8 Risk Reporting and the Role of Communication and Information	44
2.8.1 Communication and Information	44
2.8.2 Reporting	44
2.9 Company-wide Risk Management	46
2.10 Operational Risk Management in Smaller Banks	49
2.11 Operational Risk Management by Securities and Investment Firms in Austria	50
2.12 Principles for the Sound Management of Operational Risk	51
<b>3 Specific Measures of Operational Risk Management</b>	<b>54</b>
3.1 Systems: Infrastructure	54
3.1.1 General Risks – Infrastructure	54
3.1.2 Special Risks – Infrastructure	55

3.1.3	General Measures – Infrastructure	57
3.1.4	Special Measures – Infrastructure	58
3.2	Systems: Information Technology	61
3.2.1	General Risks – Information Technology	61
3.2.2	Special Risks – Information Technology	62
3.2.3	General Measures – Information Technology	64
3.2.4	Special Measures – Information Technology	70
3.3	Business Processes	71
3.3.1	Risks – Business Processes	71
3.3.2	General Measures – Business Processes	74
3.3.3	Special Measures – Business Processes	78
3.4	Staff	79
3.4.1	General Risks – Staff	79
3.4.2	Special Risks – Staff	81
3.4.3	General Measures – Staff	81
3.4.4	Special Measures – Staff	83
3.5	External Events	84
3.5.1	General Risks – External Events	84
3.5.2	Special Risks – External Events	85
3.5.3	General Measures – External Events	88
3.5.4	Special Measures – External Events	89
3.6	Legal Risk	90
3.6.1	General Considerations on Legal Risk	90
3.6.2	Special Legal Risks	93
3.6.3	Measures in the Field of Legal Risk	95
<b>4</b>	<b>Basel II: Requirements and Capital Standards in Different Approaches</b>	<b>97</b>
4.1	Introduction	97
4.2	Basic Indicator Approach	97
4.2.1	General	97
4.2.2	Capital Requirement	97
4.2.3	Critical Assessment of the Basic Indicator Approach	99
4.3	Standardized Approach	99
4.3.1	General	99
4.3.2	Capital Requirement	100
4.3.3	Business Line Mapping	102
4.3.4	Qualifying Criteria	102
4.3.5	Role of the Competent Supervisory Authorities under the Standardized Approach	103
4.3.6	Alternative Standardized Approach	103
4.3.7	Critical Assessment of the Standardized Approach and the Alternative Standardized Approach	104
4.4	Advanced Measurement Approaches	104
4.4.1	General	104
4.4.2	Qualifying Criteria	104
4.4.3	Recognition of the Risk-Mitigating Impact of Insurance and other Risk Transfer Mechanisms	108

4.4.4	Application of AMAs on a Group-Wide Basis	109
4.4.5	Authorization of AMAs by Competent Authorities	109
4.4.6	Partial Use of Several Operational Risk Approaches	110
4.4.7	Critical Assessment of AMAs	110
4.5	Capital Requirements for Covering the Operational Risk of Investment Firms	110
	<b>References</b>	113

# 1 Causes and Definition of Operational Risk

## 1.1 Introduction

*“At Unit 4, there was a ready capability for the operators manually to disable certain safety systems, bypass automatic scram trips, and reset or suppress various alarm signals. This could be done ordinarily by connecting jumper wires [...]. The operating procedures permitted such disabling under some circumstances.”*

*“Blocking the emergency core cooling system over this period and permitting operation for a prolonged period with a vital safety system unavailable are indicative of an absence of safety culture.”*

Quoted from a report of the International Atomic Energy Agency (IAEA) on the Chernobyl accident on April 26, 1986.<sup>1</sup>

As experience shows, the sure way to disaster is to consistently neglect existing risks until everybody is convinced that nothing will happen anyway – because nothing has ever happened (which is practically never true) and actually nothing should happen (which is practically always true). Due to such a lack of risk culture, major hazard and loss potentials can build up, unexpectedly materialize at some point in time and escalate to damage on a disastrous scale due to the often quoted “unlucky chain of events”. Chernobyl is an example serving as a warning: this nuclear accident had consequences on a global scale and its impact can still be measured today.

These Guidelines, however, discuss certain risks faced by banks – and a credit institution obviously cannot be compared with a nuclear power plant. Nevertheless, the introductory quote was not selected by chance since the military and nuclear technology of the past century is considered to be the origin of the concept of “operational risk”. In the field of financial services, too, operational risk is not a negligible factor: in overall terms, it is far higher than market risk for most banks and, thus, is the second biggest risk category after credit risk.

What is it actually all about? In its narrower sense, i.e. the risk involved in the operation<sup>2</sup> of an enterprise, operational risk is closer to the origins of the risk concept<sup>3</sup> than the business risks specific to banking. The hazards in question naturally are or were also linked with other types of business activities, but in several respects, a bank is not just another company like all the rest. In its intermediary function as both borrower and lender, banks have a central role to play in the economy as a whole. Therefore, the risk of mistakes, incompetence, criminal tendencies, loss or unavailability of employees, diverse process mistakes (account entries, settlement, valuation, etc.) or failures of technical systems as well as the dangers resulting from external factors, such as violence and white-collar crime, physical threats or natural disasters, and legal risks also involve the potential of corresponding effects. This potential is even multiplied by the increasing complexity of banking, e.g. the ambivalent role of

<sup>1</sup> IAEA, The Chernobyl Accident, Safety Series No. 75 - INSAG-7, Vienna, 1992.

<sup>2</sup> From Latin *operare* = work, operate, create.

<sup>3</sup> From Greek *riza*, Italian *rischio*, Spanish *risco* = cliff: our risk notion was shaped by the marine insurance sector.

information technologies in overcoming old risks and creating new ones, the expanding and changing business activities of banks, progressive globalization and automation, as well as more and more complex financial products.

The aspects described more than sufficiently justify that operational risks be treated as a separate risk category in banks; moreover, prominent cases from the recent past illustrate how banks experience serious material – or reputational – losses or may be threatened in their existence when operational risks materialize.

## 1.2 Definition of Operational Risk

Operational risk<sup>4</sup> – as the term already indicates, the potential losses associated with operating or “working” in the broadest sense – can be well illustrated by examples, but it is not easy to find a definition that is both comprehensive and functional. For this reason, the focus has long been on listing the risks not constituting operational risk, i.e. neither credit risk<sup>5</sup> nor market risk<sup>6</sup>, and thus “defining” it as the residual risk.

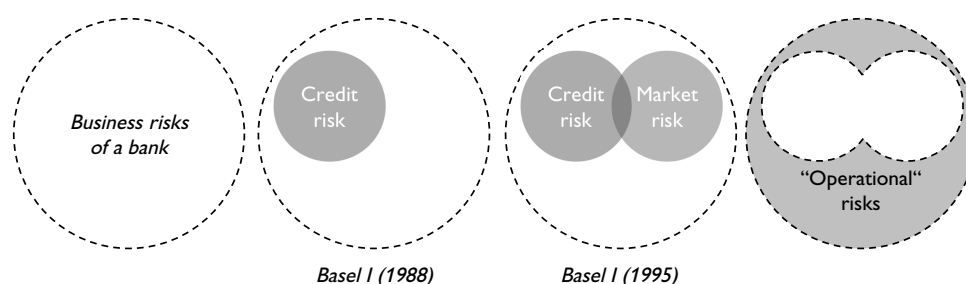


Chart 1.1: Operational Risk as “Complementary Risk” (residual risk defined by exclusion)

Apart from the disadvantages of such a negative definition for identifying and measuring operational risk, which may lead to gaps and duplication in coverage, this only provided a generic heading for a broad range of highly diverse and poorly quantifiable risks. For example, according to this definition, business risk would form part of operational risk although it constitutes the enterprise’s inherent risk of strategic management decisions and, therefore, is beyond the risk manager’s control and competence.

In June 1999, the Basel Committee on Banking Supervision<sup>7</sup> decided to highlight the importance attributed to operational risk in banks by advocating an explicit regulatory capital charge for other risks. One of the reasons for doing so was the fact that the capital held as a cushion against residual risks, including operational risk, was increasingly reduced due to the more and more accurate measurement of credit risk.

<sup>4</sup> Not to be mixed up with “operations risk” that, being the risk of errors inherent in complex systems and processes, constitutes a subset of operational risk and, for example, does not include fraud, model or serial risks (legal risk).

<sup>5</sup> The risk that debtors are unable to meet their obligations or that their credit rating deteriorates.

<sup>6</sup> The risk that adverse market movements reduce the value of positions held.

<sup>7</sup> Basel Committee on Banking Supervision, A New Capital Adequacy Framework: Consultative Document, 1999 (“CP 1”).



In January 2001, the Basel Committee narrowed down these other risks<sup>8</sup> by drafting the first definition of operational risk that was eventually finalized in a working paper presented by the Basel Committee in September 2001. Thus, the basis was essentially created for taking account of this risk category in the requirements for risk management and capital adequacy.

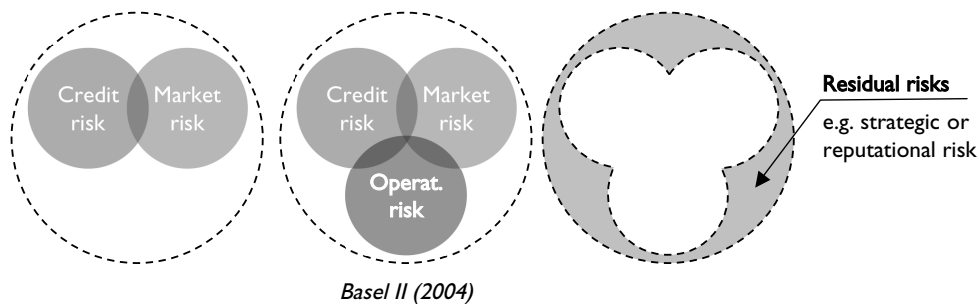


Chart 1.2: Operational Risk as a Separate Risk Category Defined Positively

In its definition, the Basel Committee focused on the causes of (potential) loss events in order to differentiate operational losses from events falling in other risk categories:

*“Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.”*

The European Commission’s Directive 2006/48/EC<sup>9</sup> which is implemented in national legislation (Austrian Banking Act – Bankwesengesetz) translates this definition as follows:

*“Operational risk means the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events, and includes legal risk.”*

Here, too, legal risk is included in the definition’s scope, while strategic and reputational risks are not explicitly excluded. Depending on the precise risk definition of a bank, this may play a significant role in considering management mistakes or reputational consequences of operation-related incidents because, by definition, operational risk management processes relate to all the risk areas covered.

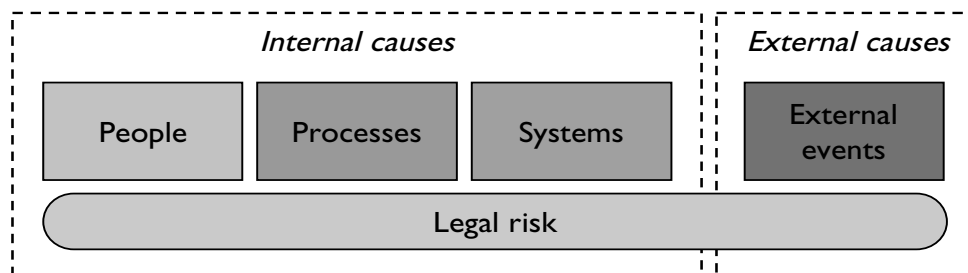


Chart 1.3: The “4-Cause Definition” of Operational Risk According to Basel

<sup>8</sup> Basel Committee on Banking Supervision, Consultative Document: Operational Risk, 2001 (“CP 2”).

<sup>9</sup> In the following referred to as “EU Directive [2006/48/EC]” (see also “Literature”).

The inclusion of legal risk (for a discussion of its definition, see chapter 3.6) is of special importance, among others, due to the fact that it is a “manifestation” of a potential operational risk and, thus, constitutes a kind of indirect cause following from one or more of the four causes of operational risk mentioned in the definition: it may result in losses depending on the way in which the legal system of a country allocates risks (assumption of risks or fault-based liability).

**Example: Interest adjustment clause.** A bank implements a provision of the Austrian Banking Act in a technically correct, but illegal manner – a court ruling on another bank reveals this process error and resulting in claims for damages. The process-related cause and the (triggering) external cause are manifested in the form of legal risk.

**Example: Employee exploitation.** The director of a branch forces the employees to work excessive overtime: this directly results in a higher error rate (cause: human factor), but also has legal implications (under labor law) – both aspects are included by the definition.

By laying down the “4-cause definition” of operational risk, a standard was created whose strength is less its previous use (it actually is the smallest common denominator of earlier industry definitions), but rather its strictly causal orientation. If applied consistently, the cause-based delimitation works quite well, not least due to the fact that other risk categories are defined in a similar way, i.e. they have well distinguishable causes: a credit risk exists as soon as credit is granted and it materializes when the credit’s repayment becomes unlikely, up to total credit loss, for reasons exclusively in the borrower’s responsibility. Market risk exists as soon as market positions are entered into and materializes when the market develops in a way reducing the value of the positions entered into – up to total loss – or, in the case of derivative instruments, for example, results in the realization of accepted obligations to an extent that can hardly be estimated.

The consistent use of an operational risk definition in a bank is of key importance no matter whether it is in line with the official definition or not. As a central element of delimitation, it is the fundamental basis for all other measures of operational risk management.

### 1.3 Characteristics and Importance of Operational Risk

Operational risks exist as soon as a company uses employees and/or systems in processes or is subject to external impacts and, therefore, they emerge long before credit or market risks are entered into for the first time. As experiences made in the past 15 years show, operational risks are a major source of financial loss in the banking sector. At a closer look, a significant share of loss events recorded by banks that are attributed to market or credit risk are actually at least related to operational risk (chapter 1.4 lists a few well-known cases). After all, it is not the consequences but the cause(s) of a loss event that, by definition, determine whether it is an operational loss event: hence, operational risks may materialize directly or indirectly through a market or credit risk.

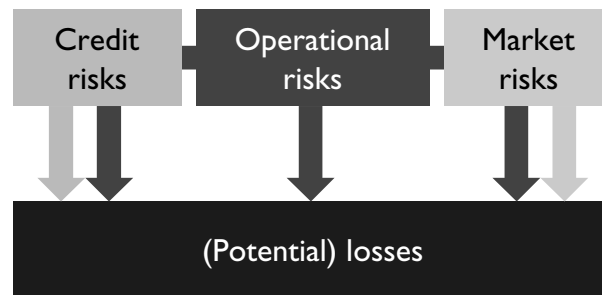


Chart 1.4: Operational Risk May Materialize Directly or Through Credit or Market Risk

Examples are business transactions performed with the intent to defraud (e.g. in the cases of Daiwa Bank and Barings, see chapter 1.4) where the loss is generated by a market risk but nevertheless caused by operational risk, namely organizational and process shortcomings or fraud. In contrast, the losses in the German Schneider affair<sup>10</sup> resulted from a default on debts, i.e. apparently a typical case of credit risk; the cause, however, also came from the field of operational risk and was related to inadequate processes for reviewing credit standings and granting loans.

In recent years, external causes have also clearly increased, both at a global level in the form of decisive events, such as the World Trade Center attacks on September 11, 2001 and the impact of SARS in Asia, and on a local scale in the case of floods, earthquakes, computer viruses, etc.

By its nature, operational risk is characterized:

- as inherent to business, i.e. inseparably linked with almost all business activities;
- as specific, i.e. its precise form and, therefore, all measures to control and mitigate it strongly depend on the specific company profile; and
- as a cultural risk because the handling of so varied and networked risks as they are summarized under the heading of operational risk is a question of a company's risk culture, i.e. its approach and practices in treating risks especially in day-to-day business.

There are major conceptual differences to credit and market risks:

- First of all, operational risk does not involve a clear relation between risk and income, i.e. higher operational risks, as a rule, do not lead to better income prospects.
- In contrast to other banking risks, a major part of operational risk is fully located inside financial institutions and it is understandable – for competition reasons alone – that banks take care not to draw attention to their own weaknesses. On the one hand, this results in a lack of event data for building an appropriately broad statistical database, which may be further aggravated by a generally bad database for certain loss event types in specific business lines. On the other hand, loss events of one bank are not nec-

<sup>10</sup> Utz, Bedeutung operationeller Risiken aus Sicht von Banken und Sparkassen, in: Eller/Gruber/Reif (eds.) Handbuch Operationelle Risiken, 2002.

essarily transferable to other banks – due to differences in business activities, practices or internal control.

- In the case of credit and market risks, risk factors, i.e. determining circumstances, and risk potentials, i.e. existing exposures, can be better differentiated due to the generally deliberate acceptance of risks. It is relatively easy to measure and, thus, control the latter risks, while it is much more difficult to establish a link between risk factors and the probability/severity of losses for operational risk.
- Very high operational losses potentially threatening the stability of a credit institution are relatively infrequent. This is the reason why some scepticism has been voiced about the statistical robustness of operational value at risk (VaR) at a high confidence level.

On principle, however, the loss potential is determined by the combination of the magnitude and likelihood of loss also in the case of operational risk – none of these “risk dimensions” alone is suitable as an objective measure of exposure, as is illustrated by a simple example:

**Example:** Which mode of transport is most dangerous? Chart 1.5 presents a simplified comparison of the potential severity of accidents (for passengers) and the frequency of accidents for some modes of transport: As a rule, passenger cars are characterized by a very high accident frequency, but only mean severity because such accidents often only involve damage to vehicles or minor injuries. For motorbikes, however, the mean severity is higher even though accident frequency is lower since severe injuries are more frequent (this is similarly true of pedestrian and bicycle accidents). In the case of aircrafts, which are considered to be very safe with regard to accident frequency, this very low frequency almost always goes hand in hand with the highest possible accident severity. The transport mode with the lowest accident frequency and, at the same time, lowest average severity is rail transport.

The combination of the two risk dimensions in the form of a simple product of two numbers (mean values of severity and frequency of damage), however, is insufficient as a risk measure. Thus, it is easy to identify the mode of transport with the least risk in the example mentioned above (for that purpose, you do not need to know exactly what “risk” means because a low accident frequency combined with a low mean accident severity is always better in comparisons). It is much more difficult to put the two risk dimensions into perspective, i.e. to translate them into a risk measure combining the influences of damage severity and probability to obtain the damage potential so that (comparative) risk assessments are possible. These, in their turn, are a basic prerequisite of risk control and targeted measures since, in practice, the key risk events hardly involve both severe loss and high probability (in such an environment, companies would not be long-lived), but rather events with most diverse combinations of loss severity and frequency. In particular, unexpected loss, which is the main focus of operational risk, lurks behind *low-frequency, high-impact (LFHI) events (tail events)*.

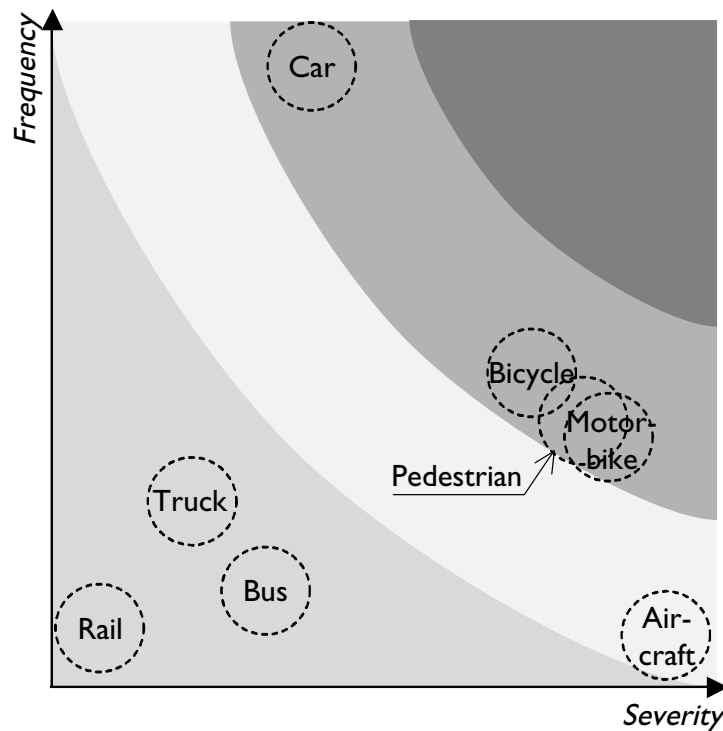


Chart 1.5: Accident Frequency and Severity for Selected Modes of Transport (graphic representation in part based on data collected by the KfV<sup>11</sup>)

The example given above clearly contains significant simplifications that impair its expressiveness and, as a result, are not permitted in operational risk statistics: first and foremost, this relates to the use of a qualitative-ordinal scale (e.g. severity of injuries) instead of a metric scale for the impact (e.g. treatment costs); therefore, each loss event is converted into a loss for the purposes of operational risk. The most significant restriction, however, relates to the fact that the example neglects that the frequency of certain accidents (i.e. multiple events) – related to a passenger – is subject to a probability distribution in addition to the probability of each possible impact for each of the transport modes identified – related to an individual accident. In fact, there is actually a **severity distribution** and a **frequency distribution** for which only the mean values have been considered so far. The product of these mean values need not necessarily reflect the actual risk (hazard to passengers) accurately, since, as a rule, a higher severity is more than compensated by its related lower probability.

In methodological terms, it would be correct to combine (convolute) the entire information contained in both distributions using statistical methods: If this is done separately for each transport mode, the desired comparative risk measure is obtained, and if this is done for a passenger, we get quantitative risk measures, i.e. an impact to be realistically expected (expected loss), as well as a higher impact that may occur with a specific statistic probability. When all

<sup>11</sup> Unfallstatistik 2003, Kuratorium für Verkehrssicherheit (2004).

that is aggregated to an overall loss distribution, the result is the risk inherent in the entire transportation system.<sup>12</sup>

With regard to the actual distribution of losses caused by operational risks in banks, we have to rely on sample surveys of descriptive statistics within the framework of actuarial (mathematical-statistical) approaches because it is hardly possible in practice to fully cover all risks that have been realized in the field of operational risk. On the basis of the characteristics of the resulting empirical loss distribution, an inductive statement can subsequently be made on the rough shape of the actual loss distribution (distribution class, estimators for expected values and variance, skewness, kurtosis) that can be used for the further calculation of the loss parameters identified.

In a typical loss distribution (chart 1.6) resulting from the convolution of severity and frequency distributions, the *expected loss (EL)* stands for those losses from operational risk events that a credit institution has to expect on an average (expected value). It has the nature of calculable costs that have to be adequately taken into account, i.e. absorbed as running costs and managed by internal control measures.

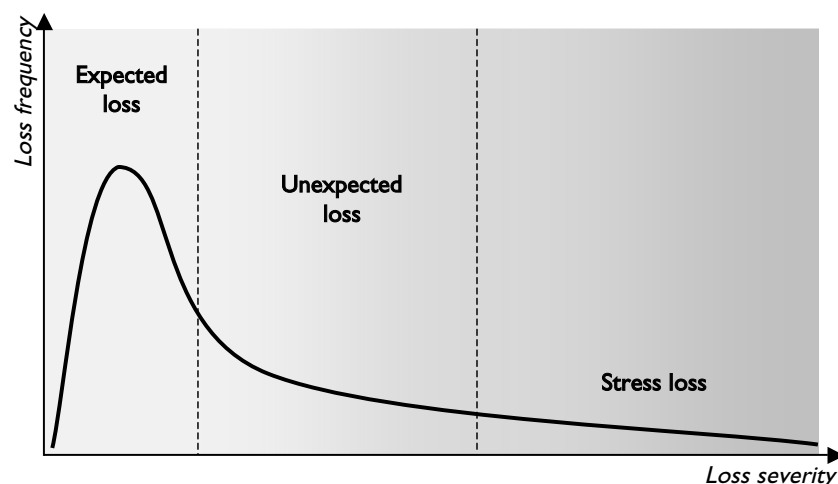


Chart 1.6: Typical Loss Distribution of Operational Loss Events

Additionally, the banks' risk prevention measures have to take account of the risk that calculated costs of expected losses cannot cover (less frequent, but higher) *unexpected losses (ULs)*. Beyond unexpected losses (above a certain probability measure, i.e. the confidence level), there are rare and extreme stress losses that play a special role in the operational risk field and can hardly be covered by capital measures. They rather have to be addressed by suitable measures (disaster and crisis management) and, if appropriate, covered by insurance contracts.

Using the relation between loss frequency and severity, a rough differentiation can also be made between the measures for managing the relevant risks

<sup>12</sup> A more in-depth risk evaluation would require a further objectivization through the use of scaling factors (such as kilometers traveled) and the consideration of the fact that not all the passengers have all transport modes available to them for all destinations and distances.

(chart 1.7): in the case of infrequent events involving low loss potentials, the most economical solution is to bear the risks, i.e. accepting them as a part of expected loss and including them in the calculated costs. If the frequency of specific loss events exceeds a certain level, risk management methods pay off serving to actively avoid such loss events – their costs naturally have to be covered by the prices. As the impact increases and the frequency of the events decreases (unexpected loss, stress loss), there is a transition from these measures to crisis or disaster management (business contingency management); to cover the material damage, risk mitigating measures are frequently used, e.g. insurance contracts.

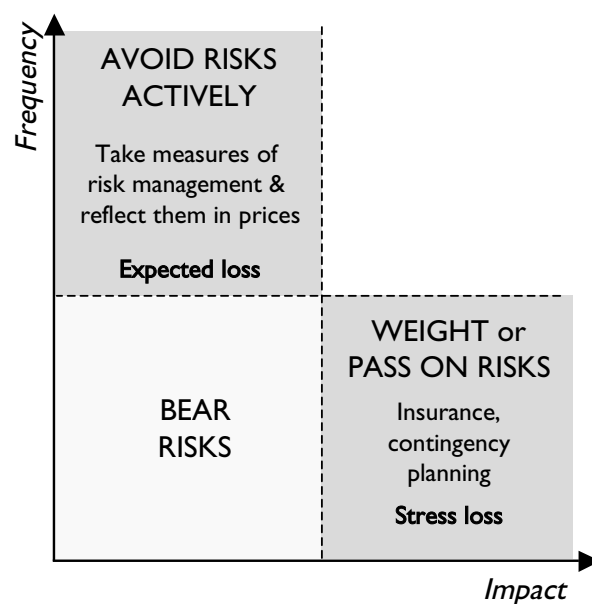


Chart 1.7: Matrix on Operational Risk Management as a Function of Impact Potential and Frequency of the Related Events (see also chapter 2). Frequent, severe loss events usually cannot be observed at a company level (“phantom risks”).

## 1.4 Case Studies

Operational risks may arise in all spheres of a bank, but they are not of the same importance in all of them. In the field of commercial banking, for example, credit risk ranks first, usually followed by operational risk and market risk, while market risk predominates in investment banking, trading or treasury, and operational risk constitutes the main hazard in fields such as asset management or retail brokerage. An overall view of the bank, however, should also take account of the fact that a relatively low importance of operational risk in one business line may correspond to a significant hazard (e.g. in the case of an accordingly high trading volume).

In the recent past, the causes of the most prominent examples of losses due to operational risks have been rogue trader<sup>13</sup> cases and, thus, are close to the

<sup>13</sup> Rogue traders are criminally minded insiders acting on their own who either stand out due to their extreme success (“risky stars”, see also chapter 3) or engage in their underhand practices for years and years without raising any suspicion.

borderline to market risk. In these cases, controls failed so that fraudulent practices of individual (seldom of several) employees (usually traders) resulted in direct losses, indirect losses due to impaired reputation and, sometimes even bankruptcy.

- There is one case of a risky star that must not be missed in any serious study on operational risk: Nick Leeson, the most famous rogue trader. In his functions of both (!) head of trading and head of settlements at the subsidiary **Barings** Futures Singapore (BFS), he was in charge of trading for customers and for own account; these essentially were arbitrage transactions under various contracts on SIMEX<sup>14</sup> and OSE<sup>15</sup> that Barings hardly considered risky. In his absolutely unacceptable double function, Leeson built up unhedged positions and had emerging losses entered into a difference account (the famous “88888-account”) that he balanced through an income account outside the audit scope of the internal audit division. The internal auditors of BFS explicitly called for a separation of Leeson’s functions which, however, the management knowingly did not implement. In the course of massive losses in Japanese share prices and the Nikkei index due to the Kobe earthquake in January 1995, Leeson’s sham hedging strategy no longer worked and SIMEX issued a further margin call for which Barings London promptly provided funds to Leeson without any further inquiries. But subsequently, SIMEX ordered audits to be performed at BFS’s and Leeson was exposed. This case caused a loss of USD 1.4 billion and, after a 230-year long life, the bankruptcy of venerable Barings Bank, afterwards taken over by ING.<sup>16</sup>
- In Germany, Jürgen **Schneider** obtained excessively high loans from more than 50 banks by means of fake balance sheets and construction documents as well as lease contracts up to 1994. He used the funds to build a real estate empire and operate a well-functioning cycle of term deposits. His financial collapse resulted in net losses of DEM 2.4 billion. In this case, the banks acted negligently and did not fully examine Schneider’s financing schemes. In part, a genuine management risk existed, i.e. wrong decisions or employees being influenced by the bank management.<sup>17</sup>
- For eleven years up to 1995, a bond trader of **Daiwa Bank** in New York had caused and hidden losses of USD 1.1 billion through non-compliant transactions and scam deals.<sup>18</sup> Daiwa did not have any appreciable management controls nor even the most simple internal controls that could have immediately exposed the fraudulent transactions. The bank became insolvent, eleven senior executives were ordered to pay damages as they failed to supervise staff.<sup>19</sup>

<sup>14</sup> Singapore International Monetary Exchange.

<sup>15</sup> Osaka Stock Exchange.

<sup>16</sup> Report of the Board of Banking Supervision Inquiry into the Circumstances of the Collapse of Barings, July 18, 1995, see <http://www.numa.com/ref/barings/bar00.htm>

<sup>17</sup> Utz, Bedeutung operationeller Risiken aus Sicht von Banken und Sparkassen, in: Eller/Gruber/Reif (eds.), Handbuch operationeller Risiken, p. 105, Schäffer-Pöschl, Stuttgart 2002.

<sup>18</sup> Asia Week of Oct. 27, 1995, see <http://www.asiaweek.com/asiaweek/95/1027/biz2.html>.

<sup>19</sup> BBC News of Sept. 20, 2000, see <http://news.bbc.co.uk/1/hi/business/933834.stm>.



- From 1986 to 1996, the chief trader of **Sumitomo Corporation** (Yasuo Hamanaka nicknamed “Mr Five Percent” due to the share of the global copper market that he controlled) built up losses of USD 1.8 billion through fraudulent copper transactions. His actions that affected the entire world copper market simply were not supervised by the bank.<sup>20</sup>
- From 1992 to 1994, German **Metallgesellschaft AG** suffered losses of DEM 2.3 billion resulting from petroleum transactions and related hedge contracts. Petroleum forward contracts of a considerable volume were hedged by means of revolving short-term contracts (oil futures) and, during the decline of the oil price in 1993, Metallgesellschaft experienced a cash-flow crisis due to margin calls. In this situation, the measures proposed by the chief trader to hedge against further price reductions (buying put options) were simply not taken and the supervisory board pushed for reducing the volumes of delivery contracts and hedge positions, which meant that the major part of the losses was actually realized. To date, the question of who is responsible for the need for the MG group’s rescue is still disputed, but at any rate, it is a case of management risk (insufficient expert knowledge of the board members) and lacking risk management.<sup>21</sup>
- The treasurer of the **Orange County** Investment Pool (1994: USD 7.8 billion) had earned substantial profits over several years by investing in repos while interest rates remained stable or decreased. However, the rising interest rate level from 1994 on, the related decline in bond prices and collateral calls resulted in enormous losses leading up to Orange County’s bankruptcy. Though this case may appear to be caused by market risks, it actually was due to a model risk and, above all, to a failure of internal and external controls as well as, in part, lacking expert knowledge and management competence.<sup>22</sup>
- **Morgan Grenfell** Asset Management, a London subsidiary of Deutsche Bank, had to be saved from insolvency by its parent company providing GBP 200 million in September 1996. Moreover, Deutsche Bank paid GBP 380 million in damages to investors after a risky star (the trader Peter Young), in excess of his authorization, had bought unlisted or little known Scandinavian shares and repeatedly revalued them with his own prices. These valuations were never scrutinized by third parties.<sup>23</sup>

This list of well-known examples could be easily expanded by adding less spectacular cases – the number of events never publicized strongly increases as the volume of losses decreases. The potential hazard of an impaired reputation that – justly or not – may materialize in the form of lost profits due to the declining trust of customers and investors must not be underrated. This is why cases generally are only made public if this cannot be avoided: in a business where money is traded against trust, there is a certain sensitivity to the reputational component of operational risk events.

<sup>20</sup> Der Spiegel 26/1996, “Mister Fünf Prozent”.

<sup>21</sup> Digenan/Felson/Kelly/Wiemert: Metallgesellschaft AG: A Case Study, see <http://www.stuart.iit.edu/fmtreview/fmtrev3.htm>.

<sup>22</sup> Jorion, Big Bets Gone Bad: Derivatives and Bankruptcy in Orange County, Academic Press, 1995.

<sup>23</sup> BBC News of April 30, 1999, see <http://news.bbc.co.uk/1/hi/uk/332462.stm>.

## 2 Methods of Operational Risk Management

### 2.1 Introduction

Risk management is not an end in itself, but a key instrument supporting the management in achieving corporate objectives. This applies, in particular, to the management of operational risk.

There is a close relation between a company's mission, its vision and general strategic orientation on the one hand, and its willingness to take risk (risk appetite, risk tolerance), risk policy and risk strategy, on the other hand. All these elements have a strong impact on corporate culture and, therefore, on values, opinions and attitudes of employees. It is decisive for the well-balanced interaction of those elements whether the focus is on formal compliance with regulatory requirements or expectations of the capital markets or whether operational risk management is fully embraced by the management and all employees in their day-to-day work.

While the basic components of a risk management system are similar, companies often significantly differ by their culture. The corporate culture of a listed, internationally active bank orientated to shareholder value, a cooperative bank rooted in a region and committed to supporting its members or a savings bank focusing on public interests differ more than the basic components of their risk management systems which always include the identification, assessment, treatment and control of risks (see chapter 2.4). It is the culture, mission and vision that shape the readiness of these companies to take risks, their risk tolerance and risk profile, and thereby the concrete form of risk management competences.

**Example:** In 2004, the **National Australia Bank** announced considerable losses from foreign exchange options. Corporate culture turned out to be a key weakness. For example, the suppression of bad news was more encouraged than open dialogue. Process guidelines and documentation were more important than understanding the essence of problems and dealing with them. The management tended to shuffle off responsibility instead of taking it. One of the consequences of this culture was that regular limit breaches of the FX desk were always approved by the direct superior and never reported to the CEO, the board and its committees. This culture fostered an environment in which the traders were able to cover up their losses successfully for a long time.<sup>24</sup>

According to the Basel II definition, the behaviour and actions of people in an organization is one of the sources of operational risk. The entire work environment is important for actually implementing, for example, a risk strategy. The employees' motivation and satisfaction with their work is essential for ensuring their identification with the corporate objectives. Sanctions are definitely an important instrument for corrective interventions that may be necessary, but they should only be one of several tools for achieving the desired behaviour in a well-balanced, preventive system of incentives. Another key element for ensuring that the actual development of a company is in line with its foundations is the design of the remuneration scheme for the management and all employees. Risk-related components should be appropriately taken into account in this context.

<sup>24</sup> PwC, Investigation into Foreign Exchange Losses at the National Australia Bank, 2004.

## 2.2 Organizational Framework Conditions

### 2.2.1 Framework

An operational risk management **framework** serves to orientate the employees to the essential objectives and components of operational risk management both during the implementation phase and ongoing operations. It includes, for example:

- objectives and benefits of operational risk management,
- definition and differentiation from other types of risk,
- classification of operational risks,
- roles and responsibilities,
- methods (components, tools) for the risk management process, and
- computer systems and IT infrastructure.

Those individual items will be discussed in greater detail in various parts of these Guidelines. Due to their organizational importance, however, the “roles and responsibilities” will be dealt with already below.

### 2.2.2 Roles and Responsibilities

The clear assignment and definition of roles and responsibilities is important and frequently part of operational risk frameworks. This distribution very strongly depends on the concrete situation in a bank or group and should therefore be carefully coordinated. It should be reviewed regularly and adjusted to changed circumstances.

The **top management** is responsible for all the risks of the bank as well as for designing and implementing its risk strategy. One of the most important prerequisites for establishing an effective operational risk management system is the support of the top management right from the start. In part, the top management itself takes the initiative in launching a project on operational risk management. However, if such a project is initiated by somebody else, e.g. by the risk controlling unit, it is of great importance for the project’s success that the top management shows active support, going beyond mere acceptance, throughout the project as well as in ongoing operations. The top management should allocate appropriate budget funds and human resources to operational risk management. The example set by the management (“the tone at the top”) has a considerable influence on the risk management and control environment. A positive attitude of the top executives to risk management as well as, specifically, to operational risk management is a prerequisite for establishing an open risk culture characterized by mutual trust.

If such a function is created – in the board of directors or at least at the level below the board – a **chief risk officer (CRO)** is responsible for implementing the risk policy adopted by the entire board. As a “sponsor”, this officer should support important projects implementing methods of operational risk management. As a rule, a CRO is in charge of approving fundamental decisions, for example, with regard to strategy or capital allocation.

The central task of the **supervisory board** is to control the management. In order to fulfil this task, it should be actively informed about the most important key aspects of projects on operational risk management right from the start. After the implementation phase, the supervisory board should

receive appropriate information on significant loss events and trends within the framework of reports covering all risks as well as information on major changes in the approach to operational risk management so that it is able to evaluate and control the management's activities in the field of operational risk management. In bigger banks, a committee focusing on the management of the bank's risks and its internal control system (**risk committee**) can support the monitoring of the overall risk situation and the management's approaches to comprehensive risk identification and control as well as the establishment and maintenance of an effective internal control system.

A centralized **risk controlling** unit set up in bigger banks has the authority to lay down guidelines and methods of risk management. Depending on the bank's size, this unit may include a separate central control function for operational risk management. It draws up bank-wide framework requirements, guidelines and procedures, coordinates activities and offers training courses. Bank groups usually have a risk control function both at the group level and in the biggest operative companies.

Committees support the integral control of risks at group- or bank-wide level. In big banks, a **risk committee** or a subordinate **operational risk committee** is in charge of discussing high-level technical issues and is to support the top management in monitoring and implementing the risk policy and risk strategy as well as in defining measures to improve the quality of risk management.

**Line management** usually is responsible for the operative implementation of the risk strategy and, hence, operative risk management. Employees working in the business lines who are specifically in charge of managing operational risks have a key role to play due to their knowledge and experiences, in particular with regard to their function as coordinators between the business lines and supervising units, such as risk controlling.

**Internal auditors** may act in an auditing, advisory and project-supporting capacity. Taking over responsibility for operational risk management or for the relevant guidelines and procedures, however, would contradict the process independence of internal auditors. In most cases, they have sound knowledge of operational risks, which should be exploited when operational risk management is implemented. For example, when systematically analyzed, internal audit reports are an important source of significant loss events that should be tapped both in the implementation and ongoing operation of operational risk management. Internal auditors can support projects on the introduction of operational risk management by providing assistance and advice. Furthermore, they can take over tasks related to reviewing the risk management system, e.g. they may schedule regular reviews and evaluations of the framework. Other items regularly examined will be the recording and assessment of operational losses and the data quality of loss databases.

Control functions focusing on specific operational risk types that play an important supporting role include, for example, the **compliance function** that is in charge of establishing a well-functioning compliance organization to prevent insider trading, manage conflicts of interest and complaints as well as monitor the transactions made by employees for their own holdings (staff transactions) and the resulting operational risks.

If there is a **works council**, it is frequently necessary to obtain its consent to measures relating to the staff. Irrespective of such a requirement, it makes sense in many cases to inform and consult the works council at an early stage. Involving the employees through their statutory representative body is an important element of a corporate culture promoting effective risk management and an efficient internal control system.

## 2.3 Step-by-Step Introduction of Operational Risk Management

It makes sense to introduce operational risk management in a phased process. This is supported by the limited resources available and the required gradual acquisition of know-how and experiences, etc. The process presented in chart 2.1 constitutes a model to be adapted to the requirements in a specific case.

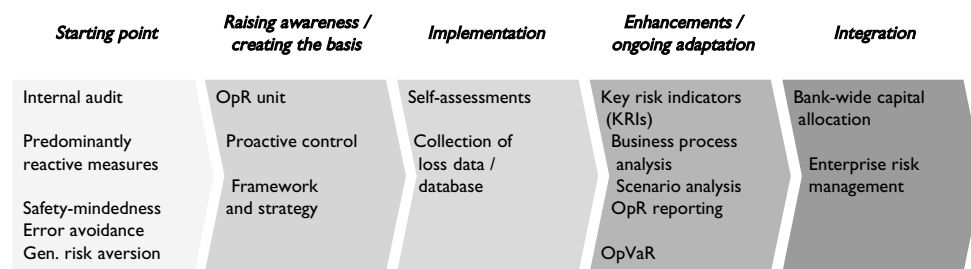


Chart 2.1: Steps in the Phased Introduction of Operational Risk Management (schematic graph)

### 2.3.1 Starting Point

Today, various organizational and technical procedures are already used to limit operational risk, also with a view to complying with a series of **legal and other regulatory framework conditions**.

To fulfil their general duty of diligence under Article 39 of the Austrian Banking Act (*Bankwesengesetz*), the managers of a credit institution are obliged to set up a risk management system and an internal control system. In this context, they specifically have to “inform themselves about and appropriately limit the risks of banking transactions and of operating the bank and give consideration to parallel risks”. The term “risks of operating the bank” used in Article 39 of the Austrian Banking Act shows that, in addition to the risks of banking transactions, operational risk already had to be considered in the past.

The managers’ obligation under company law to maintain an internal control system<sup>25</sup> that meets the company’s requirements is to be considered a further specification of their duty of diligent company management. This general duty of diligence already implies that they are obliged to establish an appropriate risk management system.

The most important measures to limit operational risk have always included the “four-eyes principle” and the separation of functions, allocation of respon-

<sup>25</sup> Article 82 of the Stock Corporation Act (*Aktiengesetz*) and Article 22 paragraph 1 of the Limited Liability Company Act (*GmbH-Gesetz*); see also Article 42 of the Austrian Banking Act (Internal Audit).

sibilities and limits, internal controls as well as reviews of the internal control system and risk management system by internal auditors, even though the view that operational risks are a separate risk category in banks has only been adopted a few years ago. The consequences of a separate treatment requested by supervisors are the development and application of specific procedures, such as the collection of loss data or self-assessment in all business lines and operational fields, the provision of regulatory and economic capital for this risk category and its integration into bank-wide capital allocation.

### 2.3.2 Raising Awareness and Creating the Basis

The first step in the process towards independent operational risk management is to raise **awareness**. Internally, major losses suffered by a bank may provide an important impetus in some cases. Eventually, however, each bank should seek to better understand its own risk profile, to actively manage operational risks on the basis of structured information, and to take preventive measures. External impulses include: the obligations resulting from the national implementation of Basel II and the incentives to apply the more sophisticated approaches, as well as well-known major loss events, such as the case of Barings Bank or the terrorist attacks of September 11, 2001. Elements of this process may include informative events and articles in an in-house newsletter or information disseminated on the intranet.

The implementation of operational risk management requires that a **definition** (see chapter 1.2) is harmonized company-wide. As a rule, this definition will be identical to the one laid down in the proposed EU Directive [2000/12/EC]. Broader definitions for internal risk controlling are possible and may include, for example, reputational risk. In this context, operational risk should also be differentiated from other risk types. The preliminary **framework** should cover and describe the elements essential for the first phase, explain the organizational structure and clarify the integration into the overall risk management of the bank or group.

### 2.3.3 Implementation

It is recommendable to start implementation by means of **pilot projects** in selected fields and, after any revisions required, proceed with the roll-out in other fields and group companies step by step. After laying the organizational basis and establishing the framework, the next step frequently is to build a loss event collection and risk inventory (self-assessment).

### 2.3.4 Enhancements and Ongoing Adaptation

As experience shows that these instruments are more difficult to implement, risk indicators, business process analyses or scenario analyses will usually only be added when the basic tools of self-assessments and the collection of loss data work satisfactorily.

Operational risk management is subject to change for two reasons: on the one hand due to the rapid development of this young discipline itself and on the other hand due to the experiences gained with this approach in the bank and the continuous changes in the bank's structures and processes that often also have an impact on the management of operational risks. Moreover,



resources in banks are usually limited so that they should be allocated in a risk-oriented manner when introducing and developing an operational risk management system. Therefore, in most cases basic processes, but also procedures that are easier to implement and well-proven are introduced at an earlier stage, while more complex procedures the bank expects to bring about improvements if implemented successfully will follow later on.

### 2.3.5 Integration into Bank-Wide Capital Allocation and Risk Management

A credit institution will reap optimum benefits from the management of operational risks, if it is ultimately integrated into bank-wide risk management.

In credit institutions, enterprise risk management<sup>26</sup> is based on two pillars: The first pillar is bank-wide management meaning that the economic capital is calculated for all risk types and allocated to all business activities. This is to create an internal system of incentives for optimizing risk-adjusted capital. The second pillar is qualitative risk management in combination with an internal control system covering all activities.

Today, the concept of risk-bearing capacity outlined below is considered to be the state of the art, especially in the German-speaking region. Like many ambitious methods in the field of risk management, the basic ideas are valid for all the banks. Smaller banks may use such procedures as food for thought and benchmarks even though they will eventually opt for simpler methods adjusted to their specific circumstances. The essential issue is that the basic idea of comprehensive risk management is implemented by all banks.

Within the framework of integrated risk control, the risk-bearing capacity refers to a bank's ability to cover against unexpected losses by means of a capital buffer that is referred to as the risk coverage capital. The central tasks of bank managers include the efficient use of tight capital resources. An essential tool for this purpose is the establishment of limits. Control at the overall bank level ultimately requires a bank-wide limit for economic capital and its distribution to risk types and business lines.<sup>27</sup> To this effect, all the quantifiable risks have to be aggregated taking into account diversification effects. As a rule, bigger banks apply a value-at-risk method in this context. Banks calculating their risk-bearing capacity should perform risk tolerance analyses at regular intervals in order to have up-to-date control data at the overall bank level.

## 2.4 Operational Risk Management as a Cycle

The management of operational risks can be described as a cycle comprised of the following steps:

- risk identification,
- risk assessment,
- risk treatment,
- risk monitoring,

<sup>26</sup> The terms "integrated risk management" and "holistic risk management", for example, are used as synonyms of "bank-wide risk management."

<sup>27</sup> See OeNB/FMA, Credit Approval Process and Credit Risk Management, 2004. The principles of the internal capital adequacy assessment process (ICAAP) according to Basel II are discussed in detail in separate guidelines.

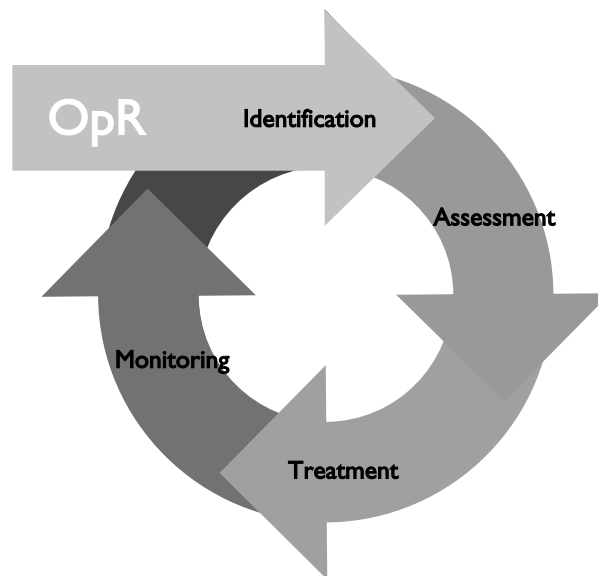


Chart 2.2: Operational Risk Management as a Cycle

## 2.5 Risk Identification and Assessment

In order to control and limit its risks, a bank first has to become aware of the potential risks. Operational risks are nothing new as such, and each credit institution has a more or less formalized internal control system including guidelines and procedures. By identifying risk sources and risk drivers, a sound “health check” – in line with the saying that “prevention is better than cure” – allows a bank to take preventive measures.

During risk identification and assessment,<sup>28</sup> banks should consider several factors in order to establish the risk profile of a company and its activities, for example:

- types of customers, activities, products,
- design, implementation and effectiveness of processes and systems,
- risk culture and risk tolerance of a company,
- personnel policy and development, and
- environment of the company.

The following tools have proven especially useful for this work:

- self-assessment (risk inventory),
- loss database,
- business process analysis,
- scenario analysis, and
- risk indicators.

These instruments are presented in greater detail in the following sections.

Together with external data, a loss database and scenario analyses form the basis for quantifying and modelling operational risk. Quantification combined with qualitative management already permits improvements in control and monitoring. Control can be further optimized if the information obtained is

<sup>28</sup> These two steps are frequently combined in practice because the methods available (e.g. self-assessment) are relevant for both of them.



used for calculating and allocating economic capital to the bank's activities so that risk-oriented bank-wide capital allocation becomes possible.

### 2.5.1 Self-Assessment (Risk Inventory)

Self-assessments aim at raising awareness of operational risks and at creating a systematic inventory as a starting point for further risk management processes as well as process improvements towards better performance.

In most cases, they take the form of structured **questionnaires** and/or (moderated) **workshops** and complementary **interviews**. Their main purpose essentially is to identify significant operational risks and then evaluate them. Using **scorecards**, qualitative evaluations obtained in a self-assessment can be translated into quantitative parameters for assessing loss frequency and severity in order to be able to rank the risks and, hence, identify the key risks. Special attention should be paid to the identification of those risks, which could endanger the survival of the institution. In graphic or tabular form, the risk portfolio can be presented as a **risk map** or **risk matrix**, respectively. A **SWOT analysis**<sup>29</sup> serves to identify and present one's own strengths and weaknesses as well as opportunities and threats.

Depending on the purpose defined, self-assessments may have a different orientation or approach:

- risk orientation,
- control orientation,
- process orientation,
- goal orientation.

Depending on the approach, the inventory focuses on one component and derives the other elements from the identification of the key component. Workshops organized in the context of operational risk management primarily aim at highlighting operational risks. Because it is usually very important for such a self-assessment to know the core processes and subprocesses of a company, the implementation of operational risk management could be preceded by a workshop identifying and evaluating processes. This could be repeated, if necessary, e.g. when important new products are introduced or when organizational changes take place.

**Structured questionnaires**, which could also be distributed through the intranet, offer the advantage of easy data recording, also in the case of big organizations with numerous organizational units. **Moderated workshops** contribute to raising awareness and communicating risks across different organizational units to a particularly high extent. In many cases, a survey (questionnaires and/or interviews) will be carried out before such a workshop. Based on the results, the workshop may then concentrate on significant risks, controls and processes.

The decision on which instruments to use also depends on corporate culture and the participation of senior management. The active involvement of senior managers as well as a participatory culture are factors contributing to the success of a workshop.

<sup>29</sup> This tool is very often used in strategic planning and can contribute to linking strategy definition (including the development of a risk strategy) and risk management.

Self-assessments may be limited to identifying and assessing **risks**, but ideally **control and risk self-assessments (CRSA)** expand risk assessments by highlighting existing or additionally required **controls** for mitigating the key risks identified. If considerable control gaps exist, CRSA workshops may develop suitable measures and action plans.

A CRSA can determine the net risk of a process, business line or activity that is relevant as a target value for measures of qualitative risk management. The net risk depends on the magnitude of the inherent risk taking account of the effectiveness of existing control measures:

$$\text{NET RISK} = \text{INHERENT RISK} \text{ minus } \text{CONTROLS}$$

For the net risk, risk treatment measures can be planned and summarized in an action plan. For this residual risk only, there is a detection risk<sup>30</sup>.

In order to be successful, self-assessments need careful **preparation**. Specifically, this means that the most suitable approach has to be chosen and the participants have to be selected and trained. Before the self-assessment, the participants should, for example, be familiarized with the operational risk definition adopted by the bank and other elements of the bank's framework for managing operational risks that are essential for understanding the system. If possible, core processes to be assigned to risks and controls within the framework of self-assessment should be identified and documented already beforehand.

Self-assessments should not be performed only once when operational risk management is introduced, but **regularly**. In practice, most of the bigger banks perform such assessments once a year. Smaller banks should schedule a review at least when major changes take place, e.g. restructuring or taking up new business lines.

Repeated self-assessments involve the danger of a certain **fatigue effect** that occurs after the first few assessments. There is, for instance, a tendency to take over the results of the previous year without critically reviewing them. This may be avoided by changing the membership of the group and by inviting employees who can contribute a new perspective to take part in the self-assessment workshop. Care should always be taken to ensure the **consistency** of the methodology and the **comparability** of the results.

Depending on the organization, **internal auditors** will be involved in self-assessment at different intensities. For smaller banks, internal auditors may be particularly helpful in the implementation phase because the internal audit function, even if outsourced, has knowledge about risks, controls and processes across the organization. In their turn, internal auditors can improve the risk orientation of audit planning on the basis of self-assessment results. In **bigger banks**, internal auditors should perform their own risk assessment independent of the management's self-assessment with a view to audit planning. On the one hand, internal auditors can obtain important information for their own work by analyzing different assessments and, on the other hand,

<sup>30</sup> The detection risk is the risk that an auditor does not detect a significant risk. The following relation applies to the audit risk that is relevant for a risk-oriented audit approach of internal and external auditors: Audit risk = inherent risk x control risk x detection risk.

they can provide an independent evaluation of self-assessment results and thereby contribute to quality control. At any rate, the risk controlling unit (or a comparable unit) has to stay in charge of the methods used and the risk owners, primarily the line managers, are to remain responsible for the management of operational risks, i.e. responsibility must not be transferred to internal auditors as this would impair their **process independence**.

### 2.5.2 Loss Database<sup>31</sup>

#### 2.5.2.1 Internal Loss Databases

Internal loss databases are used to record and classify loss events. The systematic collection of loss data within a credit institution forms the basis for an analysis of the risk situation and, subsequently, for risk control. The quality of models measuring operational risks strongly depends on the quality of the loss data recorded in the database.

An effect in collecting internal loss data is that primarily frequent loss events with low severity are recorded. (“high-frequency, low-severity events”). For this reason, the benefits of an internal loss database relate less to risk modelling, but rather to its use for improving the efficiency of processes and the internal control for those risks that should be reduced.

Internal loss databases are not suited for covering rare loss events involving high (“low-frequency, high-severity events”) and even losses, which endanger the survival of the institution. Major loss events occur extremely seldom, but may basically hit many banks. Therefore, all banks wishing to model their operational risk need to rely on external data.

The quantitative impact studies performed in the process leading to Basel II have shown that losses are concentrated on a few combinations of event-type category and business line. This reveals risk clusters reflecting the risk profile of banks. Moreover, trends can be identified over time.

Loss databases can have a very simple form. However, simple procedures rapidly reach their limits in bigger or more complex organizations when data from diverse areas or several companies have to be collated. Other organizational changes, too, may raise problems related to data consistency. As a rule, bigger institutions, therefore, use intranet-based solutions ensuring the decentralized, but uniform input of loss data.

The data fields should both meet the regulatory requirements of the approach selected and permit data analyses offering benefits internally. Please note that characteristics not recorded initially are difficult to add at a later stage. Therefore, a balance has to be found between information depth as well as benefits and costs. Examples of important data fields are:

- date (loss event, detection, entry into the books),
- severity of loss (gross loss),
- value adjustments, provisions, write-offs,
- loss-related compensations,
- event-type category,
- business line,

<sup>31</sup> For regulatory requirements, see chapters 4.4.2.3 “Treatment of Internal Data” and 4.4.2.4 “Treatment of External Data.”

- geographic location,
- company (within a group),
- organizational unit,
- description specifying significant drivers or causes of the loss event, etc., and
- reference to credit or market risk.

The data may be recorded in line with the bank's internal criteria, but the specifications have to make sure that the requirements defined for supervisory and reporting purposes are met, e.g. with regard to mapping the events into event-type categories and business lines.

It is important to have strict standards for events that must not be input (e.g. rumours or pending procedures). While rumours have to be excluded at any rate, pending procedures are a good example of borderline cases for which "viable" solutions have to be found and laid down in the standards.

A decision also has to be made on how to handle **non-monetary losses** and "**near misses**". These are difficult to evaluate, but can provide important information if recorded systematically. Specifications are also required on how to treat opportunity costs/loss of profit or profits resulting from mistakes made.

Operational losses frequently have a history and a kind of **life cycle**, i.e. they are not confined to a single point in time, but gradually become known and develop over time. The estimation of the loss may change due to new information, links between losses can become identifiable little by little or connected loss events may be spread over a period of time. Finally, compensations paid under insurance contracts or lawsuits impact the loss amount, but it often takes relatively long until the definitive loss amount is determined. As a result, loss databases should be appropriately flexible in order to take account of such changes.

It is important to avoid **duplication**, for example by recording related events that can be traced back to one root event in connection with that event.

An **approval procedure** is required for recording losses. The input of loss data should be checked and approved. As a rule, the executives of the recording units will approve the entries in line with their powers, while losses exceeding a certain level should require approval by the unit responsible for risk controlling. Furthermore, an escalation procedure should be established to ensure that losses are reported to the relevant units in line with specific criteria. In the approval procedure, it is also important to define a rule for passing on information to, and coordinating measures with, the accounting division.

There is no harmonized **non-recording threshold** below which loss data need not be stored. This threshold frequently depends on the institution's size, the business line or the methods used. While this threshold is usually rather high in investment banking, a particularly low threshold is selected if the intention is to collect data on minor, frequent loss events in order to reduce their number by targeted measures.

### 2.5.2.2 External Loss Databases

External loss data, i.e. on operational losses experienced by other banks, are collected by several data consortia and, additionally, there are a few commercial providers. Consortia allow their members to exchange loss data in a standardized, anonymous and quality-assured form.

At present, the best known data consortia are GOLD (Global Operational Loss Database) in Great Britain and ORX (Operational Riskdata eXchange association) in Switzerland. GOLD was established on the initiative of the British Bankers' Association in the year 2000. ORX was set up in 2001 and currently has 22 members. An example of a national initiative is DIPO (Database Italiano delle Perdite Operative) in Italy, a consortium founded by the Italian bank association ABI (Associazione Bancaria Italiana) in the year 2000. At the end of 2003, the membership of that consortium included 32 banks and bank groups.

The reporting threshold is EUR 20,000 for ORX, USD 50,000 for GOLD and EUR 5,000 for DIPO.

The exchange of external loss data permits benchmarking with comparable banks (peer group). In addition to their utilization in quantitative analyses and modelling, external data may also provide food for thought by raising, for example, the question whether existing controls would provide effective protection against certain events or whether reporting mechanisms are sufficient to detect such events. Information of a more qualitative nature that is obtained through self-assessments can be validated by means of external data. Thus, external data may also contribute to improving qualitative risk management.

Confidentiality among the member banks and strictly anonymous information are key factors for the development of data consortia. This may lead to restrictions with regard to information depth since geographic information, for example, might reveal the data source especially if the number of members is low.

The consistency of data recording has to be ensured. Banks should input data on comparable loss events in the same way. This should also be guaranteed within one bank. Hence, data field names should be easily understood and sufficient information should be recorded to permit data validation. By consistent data recording, data consortia fulfil an important function in ensuring comparability.

Finally, consortia and their systems have to be structured in such a way that they are flexible with a view to future developments, such as changes in categories or amendments due to new risks.

A problem related to the use of external data is their methodical classification and scaling. A loss that can be easily borne by one bank may threaten the life of another bank. Different factors may be used for scaling, e.g. balance sheet total, expenditure or income, with different factors being relevant for different business lines. However, since suitable data are only available to a certain extent, pragmatic solutions are needed in this context.

### 2.5.3 Business Process Analysis

Within the framework of operational risk management, business process analyses are used, in particular, to link processes, risks and controls in a risk

analysis. They may also have the purpose of ensuring risk-oriented process optimization.

The identification of business processes across all organizational units is a prerequisite for allocating **loss data** to processes and determining the risk for a business process. Moreover, there is a close connection between business process analyses and self-assessments. On the basis of **self-assessment**, it should be possible to allocate the significant risks and controls identified to the business processes. As a result, at least a rough business process analysis should already be carried out before self-assessment.

In a business process analysis, processes and process steps are assigned to products and process chains are examined for risk-sensitive items. For such items, **loss scenarios** can be defined. Scenarios are a mandatory element required for the approval of an AMA as well as a central input for a scenario-based AMA.

Through the **documentation** of processes and the identification of the organizational units involved in them, processes can be made transparent and improved with regard to effectiveness and efficiency.

It is recommendable to define first the processes that are especially critical with regard to operational risks and thereby prioritize them. The subsequent business process analysis should focus on these processes.

In a process map or process matrix, management processes, operative processes and supporting processes can be presented together with their interactions. Process descriptions, which are updated as necessary, facilitate communication between process owners and the employees who are process users. Important criteria are the processes' transparency, user-friendliness and up-to-dateness.

A business process analysis is a procedure requiring great efforts. It has to be maintained on an ongoing basis and must be reviewed regularly, but makes it possible to establish links between cause and effect and, due to the improvements it triggers in process management, may provide an added value.

Business process analyses are a method indispensable for the management of operational risks because business processes are a source of numerous significant operational risks. Process risks and related measures are presented in chapter 3.3.

#### 2.5.4 Scenario Analysis

Scenario analyses, which are a mandatory element of AMAs, are to identify possible high-impact events that have not occurred to date. In contrast to the collection of loss data that focuses exclusively on the past, scenario analyses emphasize future-oriented aspects of operational risk.

There is a close link between scenario analyses and **stress tests** because the empirical or analytical identification of extreme scenarios is a prerequisite for performing stress tests. These tests are used to simulate and weight the impact of different scenarios.

There is no harmonized, binding definition of the term "scenario". A scenario may be defined, for example, as a sequence of possible events and the description of possible developments leading up to these events. "What-if" questions asked in a scenario analysis shift the focus of risk assessment to the



future. Due to this future orientation, scenario analyses are an important instrument complementing loss databases that exclusively document past events.

Scenarios may be developed, for instance, along organizational units and risk factors, such as IT, processes, infrastructure or outsourcing, with risk factors being of different relevance for each organizational unit. The potential loss severity and frequency is to be estimated for the scenarios identified. Extreme events that occurred at other banks, for example, may be used for generating scenarios.

The objectives of scenario analyses performed in the context of operational risk management have both quantitative and qualitative aspects:

- Quantitative aspects:
  - complementation of data used for calculating risk capital,
  - basis for carrying out stress tests.
- Qualitative aspects:
  - insights into horizontal risks,
  - early detection of risks,
  - identification of the bank's weaknesses,
  - ideas for process optimization.

Scenario analyses can follow a top-down or a bottom-up approach. In a **top-down approach**, managers and other experts identify possible operational loss events that range from losses occurring every day to stress events. The **bottom-up approach** may start with a detailed process analysis or risk assessment and assign probabilities and loss severity to possible individual events. Big commercial banks tend to apply a top-down approach.

An essential aspect is the utilization of expert knowledge. In addition to the management of the business lines, in particular, the heads of staff units, such as risk management, IT, legal affairs, insurance or internal auditing, should be involved.

Information may be collected during workshops, by means of questionnaires or in interviews. It is important to design the instruments used in such a way that the repeatability of the process is ensured. Therefore, attention should be given to consistency in the preparation process and the utilization of results in further process steps.

Within the framework of **early-warning systems**, scenarios are used to collect (uncertain) information on significant internal and external influences. This information is used to assess potential effects on the company's strategies and activities. As a rule, the time horizon goes far beyond the timeframe of normal planning.

In an open, quality-oriented form, scenario analyses are a suitable instrument for identifying medium- to long-term risks in a bank and for bringing risk potentials in line with the strategic orientation. In connection with approaches of system-oriented "network thinking", scenario analyses live up to the complexity and dynamism faced by banks today and tomorrow. Thus, scenario analyses may be an important component of a bank's early-warning system and strategy development.

Scenarios outline pictures of the future or plausible explanations on possible “futures”. They are neither forecasts nor do they draw up utopias. They primarily focus on identifying influencing factors and interrelated effects.

The “**scenario funnel**” illustrates the spread of scenarios and the spectrum of conceivable future situations widening under the influence of incidents and interventions over time.

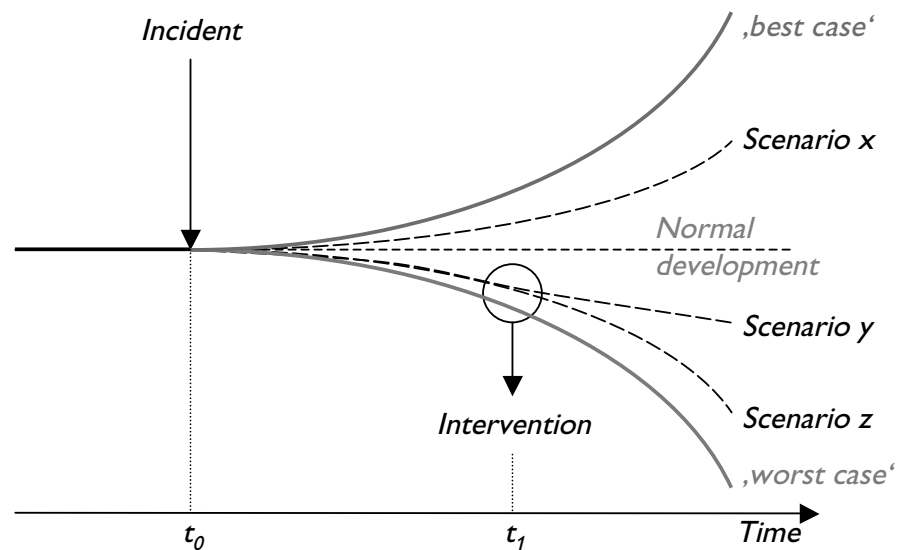


Chart 2.3: The “Scenario Funnel:” The Possible Further Development in the Wake of an Incident Corresponds to all the Scenarios Ranging from Best to Worst Case

### 2.5.5 Key Risk Indicators (KRIs)

Key risk indicators provide information on the risk of potential future losses. They should make it possible to identify areas with elevated risks early on and to take appropriate measures. Thresholds (“triggers”) may be defined for KRIs. They permit statements to be made on trends and can serve as indicators in an early-warning systems, e.g. in combination with a traffic-light system (red, yellow, green).

Examples of KRIs are:

- staff fluctuation rate,
- days of sickness leave,
- hours of overtime,
- number and duration of system failures,
- internal audit findings,
- frequency of complaints,
- wrong account entries.

In addition to risk indicators, the following related indicators are sometimes mentioned:

- key control indicators (KCIs),
- key performance indicators (KPIs),
- key management indicators (KMIs).

The application of KRIs, however, involves several problems. For example, difficulties with regard to classification and, hence, comparability already



occur frequently within one company and all the more among several enterprises.

The measurement frequency is determined by the response time required and the expected loss severity. Those who do not measure enough may overlook a risk driver and have to bear a resulting loss. Those who measure too much have to accept inefficiencies and maybe false alarms. Timely measurement is critical for response time, with different measurement times being appropriate for different indicators. Thus, the staff fluctuation rate may be measured at longer intervals without losing information, while critical systems need to function continuously so that their availability has to be monitored on an ongoing basis.

Numerous different risk indicators are frequently defined specifically for a company or business line. Many banks have hundreds or even thousands of indicators. This makes it very difficult to aggregate the information so that it still makes sense for higher management levels.

#### **The Key Risk Indicator (KRI) Study**

*The Risk Management Association (RMA) and a consulting company active in the field of risk management have examined the use of formal KRI programs in a study carried out in 2002. According to the study, 13% of the 76 participants used KRIs.*

*Subsequently, the two partners conducted another study on KRIs together with several international banks. The nine main participants submitted more than one thousand KRIs to the project with the aim of having them evaluated and making a library of indicators accessible to the participants on the internet for comments and benchmarking.*

*The study was based on a 3-dimensional matrix with the elements "business function", "risk categories" and "business lines". A combination of these three elements is called a "risk point".*

*Due to the broad participation, the study generates great interest among those responsible for operational risk management in bigger banks. However, exaggerated expectations should be avoided with regard to the KRIs. The result will most likely not be a small "library" of indicators that are suitable for all banks as there are too many differences both among and in banks. The development of useful indicators is a process of trial and error. But the structured exchange of experiences may provide helpful hints and contribute to avoiding dead ends.*

### **2.5.6 Quantification of Operational Risk**

Models for quantifying operational risk are currently still in a relatively early stage of development. Basel II has provided a decisive impetus to the development of appropriate models. "High-frequency, low-severity" and "low-frequency, high-severity" losses involve very different modelling requirements. This means that, as a rule, there will not be only one way of quantifying operational risk. Rather, it is necessary to find a mix of methods corresponding as well as possible to the bank's risk profile.

The procedures that may be used to calculate the regulatory capital requirement for operational risks are presented in chapter 4. Here, several concepts for quantifying such risks are explained.

The **value at risk (VaR)** of an asset position or portfolio, as it is used in the control of market or credit risks is the monetary expression of the loss in value not exceeded with a certain probability "a" (confidence level) in a defined period of time (holding duration).

The advantages of the VaR concept are that this parameter can be well interpreted and used for different types of risks and at various aggregation levels (individual positions, business lines, portfolios, entire banks) with the possibility of taking account of diversification effects due to the risk combination depending on the method used to calculate VaR.

The adaptation of the VaR concept to the quantification of operational risk, however, raises considerable difficulties. A major weakness of the VaR concept is that VaR does not provide any information on the amount of the extremely rare, extremely high losses beyond VaR. In the context of operational risks, however, extremely infrequent, life-threatening risks are important and not frequent low-severity loss events for which an extensive range of well-proven control measures is available.

A shortcoming of VaR with regard to stress losses is the uncertainty about the extent to which a loss exceeding VaR can differ from VaR (“how bad is bad?”). Alternative risk measures taking account of the distribution’s tail, such as conditional VaR, tail VaR and expected shortfall, are better suited to the specific distribution of operational risks.

The **conditional VaR**<sup>32</sup> takes account of all values below a specific level, e.g. below the 0.1% quantil, to calculate the expected value. While VaR does not say anything about the possible height of a potential loss, the conditional VaR is the expected value of (100-a)% worst cases and, hence, of the particularly interesting stress losses. The conditional VaR, frequently also called “**expected shortfall**”, is the sum of VaR and the mean excess in the case of excess losses and, as a result, expresses a conditional expectation related to VaR. It can be interpreted as the average maximum loss in cases exceeding the confidence level.

The **extreme value theory** (EVT) offers methods for modelling “fat tails” or “heavy tails” of a distribution (“let the tails speak for themselves”). In the context of operational risks, interest focuses on stress losses about whose distribution the VaR approach does not provide any information.

The VaR of market risk is usually based on the assumption of a normal distribution. This assumption considerably facilitates calculations and in most cases, provides a good approximation to the actual distribution. In the case of operational risks, however, the distribution has a right skew. Within the EVT, the generalized extreme value distribution (GEV) and the generalized Pareto distribution are more suitable statistical instruments.

“Classic” EVT describes the distribution of maxima and minima of a sample. The GEV represents the distribution of normalized maxima. After appropriate normalization, there are three possibilities for their asymptotic distribution: the Gumbel, Frechet and Weibull extreme value distributions.

Using the so-called **peaks-over-threshold (POT) method**, “moderately” extreme observations within a sample can be used to infer the properties of the extreme areas of a distribution not covered by the sample. Thus, this estimation technique makes it possible to model the distribution of extremes above a defined high threshold. The excess values are modelled using

<sup>32</sup> Also called “tail value at risk” (especially in the insurance sector), “mean excess loss” or “mean shortfall.”

generalized Pareto distributions, while the frequency of excesses is represented by Poisson distributions.

The insurance sector is familiar with similar modelling tasks in the field of non-life insurance, in particular when insuring against major damage. Their value is also mainly modelled using Pareto distributions and their frequency by means of Poisson distributions, while lognormal distributions are applied to basic damage rates.

Another problem in the modelling of operational risks is the integration of qualitative and quantitative data. Here, fuzzy logic methods and so-called Bayesian belief networks may be helpful. An advantage of these two methods is that they also are able to process and quantify expert knowledge so that it can be used for modelling.

**Fuzzy logic**<sup>33</sup> allows for a mathematical description of fuzzy data sets. It cannot replace quantitative measurements, but it allows for calculations on subjective evaluations and expert knowledge, e.g. gathered in self-assessments. Fuzzy logic is especially suited for complex multifactorial systems. Moreover, it permits the consideration of incomplete or verbal, non-numeric information in the quantification of risks.

An unambiguous dichotomic classification means that process errors are tolerated up to a specific number and are considered unacceptable beyond that limit. But why, for example, should 100 process errors be acceptable and 101 unacceptable? Instead of a clear-cut delimitation (big versus small, low – medium – high or poor – sufficient – good), fuzzy logic allows the partial assignment to different classes (fuzzy sets) by means of membership functions.

**Bayesian belief networks** are another technique for integrating qualitative data in the form of subjective beliefs and insecure knowledge into the quantitative modelling of operational risks. An advantage they offer is that they illustrate cause-effect chains that are of decisive importance for the management of operational risks. They can be applied to support scenario analyses where cause-effect relationships are important and the subjective evaluations of experts should be used due to the future-oriented nature of these analyses.

A concept related to fuzzy logic are **artificial neural networks**. Neural networks – similarly to the brain – are made up of a multitude of neurons that are networked through weighted links. The neurons are processors receiving signals as inputs and generating outputs transferred to other neurons. An essential characteristic of neural networks is their ability to learn, which is reflected in the model by the adaptation of weightings. They are primarily suitable for solving classification and forecasting problems. While neural networks are sometimes also mentioned in the context of operational risk modelling, their practical relevance is rather low in this field. In risk management, banks have used neural networks, for example, in the field of credit rating.

A statistical method used in cases of low data availability is **bootstrapping**, a resampling technique for improving estimates. The repeated modifi-

<sup>33</sup> This branch of mathematics or, more specifically, set theory, was founded by Lofti Zadeh in 1965. For the application of fuzzy logic in credit rating, see OeNB/FMA, Rating Models and Validation (2004), p. 38 ff.

cation of the data allows the evaluation of the statistical error of a hypothesis. In contrast to Monte-Carlo simulations, the simulated data sets are generated from the data themselves.

### 2.5.7 Exemplary Approaches to Calculating Regulatory Capital

In a working paper dated September 2001, the Basel Committee described three main methods covering a broad range of the requirements of advanced approaches that, therefore, can serve as examples for the development of one's own models. Although they were not included in the final version of the New Basel Capital Accord, they still are showcase examples of possible model types.

In concrete terms, the internal measurement approach (IMA), the loss distribution approach (LDA) and the scorecard approach are mentioned.

#### 2.5.7.1 Internal Measurement Approach

The internal measurement approach (IMA) divides business activities of credit institutions into individual business lines and defines loss event types. The EU Directive [2006/48/EC] lays down the loss event types (event-type categories and definitions) presented in the Annex.

For each combination of business line and loss event type, an exposure indicator (EI) is to be identified (e.g. fixed assets, transaction volume) that constitutes a measure of potential losses in this field caused by operational risks.

Based on the findings for the banks' internal loss data, the probability of a loss event (PE) and the loss for a given event (LGE) are determined. Moreover, a fixed, stable relation is assumed between expected and unexpected losses (factors). The product of the three parameters EI, PE and LGE constitutes a measure of the expected loss (EL) which is multiplied with the relevant factor to obtain the unexpected loss and thus the capital requirement. For each business line/loss type combination, this loss is calculated separately and then all the loss values are added up.

As a result, the formula for calculating the regulatory capital requirement is:

$$\text{Capital requirement} = \sum_i \sum_j \gamma_{i,j} \cdot EI_{i,j} \cdot PE_{i,j} \cdot LGE_{i,j}$$

where:

i = business line

j = loss event type

$\gamma$  = gamma factor of the relevant combination

EI = exposure indicator

PE = probability of loss event

LGE = loss given event

The gamma factor ( $\gamma$ ) indicates the capital requirement for the business line i and the loss event type j due to the expected loss. It has to be specified by each bank itself and checked by the competent authority. Thus, the sum of the individual capital requirements per business line/risk type is the bank's overall capital requirement for operational risks.

### 2.5.7.2 Loss Distribution Approach

The loss distribution approach is based on the assumption of statistical distribution shapes for operational loss events. In contrast to the internal measurement approach, however, the expected and unexpected losses are determined without estimating a gamma matrix but by identifying loss distributions on the basis of historical internal and external data series from which an overall risk indicator (value at risk) can be inferred.

For this purpose, the categorized and adjusted data sets are first used to model the loss severity and frequency distribution for each business line/event type combination and then summarized in an overall loss distribution by means of Monte-Carlo simulation or other statistical methods (e.g. Panjer's algorithm). This overall loss distribution is the basis for determining the required capital charge.

### 2.5.7.3 Scorecard Approach

This approach is based on the idea of controlling the capital covering operational risks by means of scorecards. Using different methods<sup>34</sup>, specific risk indicators forming the basis of the scorecard are calculated for each business line at regular intervals. The risk capital initially calculated for operational risks (initial capital) is continuously adjusted to the current risk profile and risk control environment by means of scorecards that include a series of indicators used as estimators for special risk types.

This involves not only quantitative, but also qualitative criteria that can provide risk management with insightful information on the assessment and control of potential risks. The data generated are objectified and validated by means of historical internal and external loss data.

The focus may be on the level of individual business lines or the entire bank. The scorecards are intended to bring a forward-looking component to the capital calculations and to reflect improvements in the risk control environment that reduce both the frequency and severity of losses.

## 2.6 Risk Treatment

The basic management elements for coping with identified and valued operational risks are:

- risk avoidance (strategy: "not taking every risk");
- risk mitigation (strategy: "intelligently minimizing risks in their development");
- risk sharing and transfer (strategy: "intelligently passing on risks to third parties"); and
- risk acceptance (strategy: "deliberately taking certain risks in a targeted way").

The primary field of application of these alternatives results from the risk matrix according to chart 1.7 (chapter 1.3) following the bank's individual risk profile. In part, a certain effect can be achieved by different methods, while

<sup>34</sup> Examples: Interviews and expert surveys, SWOT analysis, self-assessment, brainstorming, risk identification matrix, brainwriting, synectics, Delphi method, analytic search methods, morphological techniques.

some measures are not suitable for certain risks. Frequently, possible measures also are interconnected. The choices made essentially depend of the effectiveness of the measures, their cost and the time required until they become effective.

#### **2.6.1 Risk Avoidance**

In a cost-benefit analysis, a bank should opt for risk avoidance if the expected margin of activities is lower than the expected risk cost taking account of all the risks. Such activities should be abandoned or not be launched in the first place.

Such a decision has to consider several aspects, such as time horizon, available specialized expertise, strategic objectives and reputational risks.

#### **2.6.2 Risk Mitigation**

The objective may be a cause-oriented reduction of **loss frequency** or an effect-oriented reduction of **loss severity**. Both objectives can be supported by internal control activities. Additionally, risk sharing or complete risk transfer are suitable options for reducing loss severity.

The tools of risk mitigation mainly include a multitude of organizational safeguards and control measures within the framework of an internal control system:

- guidelines and procedures,
- separation of functions and “four-eyes principle”,
- need-to-know principle (access control),
- physical access control,
- coordination and plausibility checks,
- limit management,
- inventories, and
- disaster recovery and business continuity planning.

The establishment of such controls should be evidenced in a system and procedural documentation, for example, in the form of frameworks, guidelines or instructions, but also their implementation should be appropriately documented. The key principles of the separation of functions and the “four-eyes principle” are supported, for example, by job descriptions as well as the allocation of responsibilities and powers. Preventive controls embedded in business processes are particularly efficient. Informal controls play an important role in all organizations. The related decision should be made deliberately, and its justification should be traceable.

#### **2.6.3 Risk Sharing and Transfer**

Risk sharing or transfer is mainly of interest if a risk can not or only inadequately be reduced by internal controls or if the cost of controls is higher than the expected loss. Another condition is that, in comparison with the company’s risk appetite, the risk is so high that it cannot simply be accepted.

Important instruments of risk sharing and/or risk transfer are insurance and outsourcing of activities and functions. Very careful examinations are needed to see whether the desired effect can be fully or only partly achieved



and whether undesirable effects are possible. Thus, there are cases where only risk sharing is possible instead of a full risk transfer or where circumstances change over time that also shift the relation between the risk borne by the company itself and by a third party. Owing to different deductibles, insurances allow for a differentiation with a view to risk appetite and risk profiles of companies and their individual activities. In the case of outsourcing solutions, undesirable effects on the risk profile are frequently overlooked because the risk effects often are only indirectly related to the purpose aimed at.

### 2.6.3.1 Insurance

There should be close cooperation between the risk controlling unit responsible for operational risks and the unit in charge of taking out insurances in the company. In some banks, the operational risk unit is put in charge of insurances against operational risks. At any rate, it makes sense to develop an insurance concept as a basis for taking out insurances. Moreover, there should be regular coordination with risk policy and risk strategy.

Examples of typical insurance products offered for operational risks in banking are:

- property insurance,
- business interruption,
- computer crime,
- bankers professional indemnity – mistakes made by employees,
- directors and officers liability – breach of a duty of diligence by directors and officers,
- employment practices liability,
- economic crime,
- unauthorized trading, and
- vault and transport of cash.

A **bankers blanket bond** offers comprehensive coverage against loss due to diverse risks, such as fraudulent and other criminal acts of employees, forgery of documents, burglary or robbery on the bank's premises or during transports and securities churning.

Another category of insurance products discussed in the context of operational risks are **multi-peril basket products**. In comparison with peril-specific products, they offer more comprehensive coverage and are intended to help avoid overlaps and gaps. To date, there has been both little supply and demand for products tailored to the operational risks of financial institutions. But this might change due to improving data availability, progress in the measurement of operational risks and changes on the insurance market.

With regard to **terrorism risk** that frequently used to be included in property and business interruption insurance before the recent disastrous major attacks, specific solutions were developed in several countries, especially after the attacks of September 11, 2001. One of these solutions is the **"Austrian Insurance Pool for the Coverage of Terrorism Risks"** established by Austrian property insurers that started to assume liability for such risks on January 1, 2003.

In the context of the transfer of operational risks, risk managers are highly interested in the topic of **alternative risk transfer**. Here, the focus is on highly customized, company-specific solutions that include mainly self-insurance and securitization elements and permit the transfer of risks that are not or only inadequately insurable otherwise. In contrast to classic products, the insurance component is less strong. Alternative risk transfer mechanisms include instruments such as captives, rent-a-captive concepts and finite-risk solutions.

A **captive**, as an alternative in risk transfer, is a group-owned insurance company that insures certain risks of other affiliated companies. As a form of self-insurance, captives serve to balance the risk within a group of companies. A captive may be active both as a direct insurer and reinsurer. Small and medium-sized enterprises have the possibility of renting the infrastructure of a captive ("**rent-a-captive**"). The benefits include direct access to the opportunities offered by the reinsurance market and the coverage of low-frequency, high-severity risks for which the insurance market does not offer any products at all or only products with low coverage. Please note that under an AMA, insurances by captives can only be taken into account to a limited extent (see chapter 4.4.3).

**Finite-risk insurance or reinsurance solutions** combine risk financing and risk transfer with the focus on risk financing. Under this solution, a company pays contributions to a fund during a contractual term of several years. In the individual periods, loss fluctuations are offset so that risks and results are balanced over time.

In August 2003, the Joint Forum of banking, securities, and insurance supervisors<sup>35</sup> published the paper "**Operational risk transfer across financial sectors**"<sup>36</sup> mainly discussing risk transfer by means of insurance.

The report states, for example, that one of the difficulties in developing insurance products for operational risks beyond traditional products for specific risk types relates to the assessment of a bank's operational risk profile since it depends on the loss history, internal control environment and various forward-looking factors. The related uncertainty raises the price for products covering, for example, a broad range of operational risks so that supply and demand remain small in spite of the interest in such products.

From the supervisors' perspective, it is important in both the banking and insurance sectors that enterprises clearly understand in how far new and "alternative" products actually transfer operational risks and which risks, including risks of a legal nature, are connected with these instruments.

### 2.6.3.2 Outsourcing

In the past years, the **permanent** outsourcing of **key** activities or functions to other companies has considerably increased in importance in the banking

<sup>35</sup> In addition to the Basel Committee on Banking Supervision, the International Association of Insurance Supervisors (IAIS) and the International Organization of Securities Commissions (IOSCO) are members of the Joint Forum.

<sup>36</sup> Joint Forum, Operational Risk Transfer across Financial Sectors, BIS 2003.



sector. Outsourcing, however, involves several specific risks so that banking supervisors give appropriate attention to this issue.

The most important aim of outsourcing is cost reduction. Another advantage may be higher process quality and lower operational risks as compared with performing the related activities internally. In addition to cost and efficiency aspects, risk mitigation through risk sharing or transfer may be a goal, in particular, of long-term, strategic partnerships.

At first glance, outsourcing solutions apparently result in “shuffling off” the risk related to the relevant activities. In fact, however, the way in which the risk situation of a credit institution is changed by outsourcing has to be carefully studied on a case-by-case basis:

- At any rate, outsourcing always gives rise to a **business partner risk**, i.e. the risk that the business partner does not fulfil the obligations under the outsourcing agreement. The causes may range from quality problems (process or system failures or mistakes made by employees of the outsource provider) and contractual disputes to the partner’s bankruptcy. As a consequence of such problems, the services outsourced may not be rendered in the quality required, only to a limited extent or, in extreme cases, not at all.
- In addition, account has to be taken of **legal risk** which may arise from usually complex contractual relations between a credit institution and its outsource provider. Fuzzy provisions governing the duties of the outsource provider or liability issues may lead to protracted legal proceedings to clarify who is responsible for a loss event. Ultimately, the credit institution itself may even have to bear the loss in full or in part so that, in fact, conventional system or process risk was only replaced by a special legal risk without improving the risk situation of the institution.
- The **risk of losing control of core processes** finally results from inadequate secondary obligations of the outsource provider. If the outsourcing credit institution is not given adequate control, information and auditing rights beforehand, a kind of “black box” or “blind spot” emerges for risk management in the field outsourced. Thus, the quality of the processes outsourced cannot be appropriately assured nor verified. This highly unsatisfactory situation could ultimately even mean that the overall level of operational risk rises without the credit institution being aware of this fact.

These problems need to be borne in mind when outsourcing activities so that the credit institution remains in a position to assess its risk situation and take appropriate measures to limit risks. This includes the consideration of the following aspects:

- How high is **dependence** on outsource partners and which options exist for responding to any failure of the business partner (e.g. by outsourcing to a second partner, rapid reintegration of the activities concerned)? In this context, exposure to concentration risks (increasing dominant position of individual outsource providers) should be considered. In particularly critical areas (activities or functions of special importance for maintaining busi-

ness operations), business contingency plans<sup>37</sup> and fallback solutions may need to be provided; it is also recommendable to plan exit scenarios in advance. A specific question to be answered in this context is whether the know-how and skills required will still be available within the credit institution after outsourcing.

- Are the **contractual relations** between outsource provider and credit institution regulated in a sufficiently clear and comprehensive manner so that issues related to the scope of services, availability, confidentiality, etc., need not be clarified later on when problems have already cropped up? For the detailed regulation of such issues, service level agreements (SLAs)<sup>38</sup> are recommendable that can be adapted to the outsourcing case in question with regard to substance and scope. Further aspects to be considered when drafting contracts are modalities of contract termination by either party as well as issues of data protection and data security.
- Has the outsourcing company adequate **control rights** for assessing the situation in the fields outsourced? Possible options range from appropriate reporting lines to information, inspection and access rights and regular external audits. Moreover, measures have to be taken to ensure that the outsourcing of company parts or functions does not hamper or restrict the supervisor's activities.

In February 2005, the Joint Forum published the paper “**Outsourcing in Financial Services**”. It describes developments in the practice of financial institutions and their motives for outsourcing, trends<sup>39</sup>, regulatory developments, important risks related to outsourcing, etc.

The risks mentioned include strategic risks (e.g. the outsource provider might pursue strategic objectives inconsistent with the ones of the outsourcing credit institution), reputation risks (due to poor quality or services inconsistent with the credit institution's overall standards), compliance risks (e.g. with regard to data protection, consumer protection or similar legislation), country risks, counterparty risks, contractual risks (including the ability to enforce the contract in foreign legal systems) as well as concentration and systemic risks. Among the operational risks due to outsourcing, the consultation paper lists technology failure, fraud, error and the risk that outsourcing firms might not undertake inspections for cost or other reasons.

The paper proposes nine high-level principles: seven cover the responsibilities of regulated entities when they outsource their activities and two relate to the role and responsibilities of regulators and supervisors.

The multitude of risks related to outsourcing illustrates that such complex issues – comparable to the topic of securitized products<sup>40</sup> – require a comprehensive risk analysis. The results should also be input into the identification

<sup>37</sup> See also the explanations in chapter 3.1.4 “Special Measures – Infrastructure.”

<sup>38</sup> Service and performance specifications agreed between service provider and client on the basis of objective, quantitative criteria.

<sup>39</sup> Business processing outsourcing (BPO) and off-shoring, i.e. outsourcing beyond national borders, are identified as two major trends.

<sup>40</sup> See OeNB/FMA, Best Practices in Risk Management for Securitized Products (2004), in particular p. 20 ff.

and assessment of operational risks. An isolated analysis would be likely to neglect significant components and relations.

In April 2004, the Committee of European Banking Supervisors (CEBS) issued a consultation paper on **“High Level Principles on Outsourcing”**. An important element of this paper is the definition of outsourcing proposed:

*“Outsourcing is the supply to an authorised institution by another entity (either intra-group or independent third party) of goods, service or facilities on a structural basis (i.e. the contractual supply of goods, service or facilities that form part of the business processes and which are necessary to support the provision of banking or other financial services). The supplier may itself be an authorised or unauthorised entity.”*

The paper also contains principles designed for outsourcing institutions and supervisors.

The European Directive on markets in financial instruments (2004/39/EC) adopted on April 21, 2004, which applies both to banks and investment firms, also includes provisions on the outsourcing of important operational functions (Article 13 (5) of the Directive). This must not be undertaken in such a way as to impair materially the quality of internal control and the ability of the supervisor to monitor the firm’s compliance with all obligations. This Directive has to be transposed into national law by October 2006.

#### 2.6.4 Risk Acceptance

As a rule, risk acceptance depends on a cost-benefit analysis or weighting of expected income versus risk. A rational reason for accepting risks would be that the expected loss is lower than the cost of management activities to mitigate the risks.

It is recommendable that such decisions are systematically prepared and documented in a suitable form especially when the amounts involved are rather high. Systematization can be achieved by using a risk matrix (see chart 1.7 in chapter 1.3). Criteria, such as thresholds, and decision-making processes, including escalation procedures, should exist for accepting risks.

### 2.7 Risk Control

The monitoring of the entire risk cycle considerably contributes to its effectiveness. In particular, this is to reveal weaknesses and improvement measures.

On the one hand, there should be ongoing controls embedded as far as possible in business processes that should be performed by all employees within the framework of their tasks. On the other hand, there should be separate inspections by several internal and external entities. In combination with provisions on banking supervision, the internal audit unit, supervisory board as well as auditors and certified public accountants constitute essential safeguards against the acceptance of life-threatening risks. In spite of partly differing tasks, all the parties involved should aim at actively cooperating, in particular, to avoid the emergence of control gaps.

Internal audit has several tasks in operational risk management that are explicitly laid down in the EU Directive [2006/48/EC]. In banks applying the standardized approach, for example, internal auditors have to examine the

allocation of operational income to individual business lines. In AMA institutions, internal and/or external auditors have to review the procedures and methods of operational risk management as well as the quality of entire risk management.

### **Continuous monitoring (in-process monitoring)**

Employees should not delegate the continuous monitoring of process quality to internal auditors or superiors. If possible, this task should be integrated into the processes and carried out as a part of their responsibilities. Here, process and risk owners play a particularly important role as does the establishment of incentive schemes motivating employees to continuously fulfil their responsibility and, if necessary, providing sanctions for failures.

### **Separate inspections (process-independent monitoring)**

Separate inspections can take the form of case-by-case and system audits. They may be performed by internal auditors or external auditors, for example within the framework of the statutory audit of annual accounts.

Some banks take account of internal audit information – e.g. in the form of audit scores for a business line or function – in capital allocation and thereby provide an incentive for improving the internal control system.

Monitoring in the form of internal or external audits can only fulfil its function if there are regular follow-ups. A follow-up mechanism ensures that deficiencies found are eliminated and agreed measures and recommendations are implemented in time. Factors essential for effective monitoring are the adequate support of internal audits and an active interest in external audit findings by the management and supervisory board.

## **2.8 Risk Reporting and the Role of Communication and Information**

One of the objectives of modern risk management is internal and external **risk transparency**. Open, target-oriented communication, rapid and reliable information and reporting contribute to achieving this objective.

### **2.8.1 Communication and Information**

Various organizational units of a bank need different types of information on risk management. Therefore, an element of effective risk management is regular reporting on the risk situation (in appropriately aggregated form) to the level responsible as a basis of decision-making as well as to monitoring levels (supervisory board, internal audit) and ad-hoc reporting in the case of significant events or changes in the risk situation.

It also depends on the control culture of a company whether communication is mainly limited to reporting to higher levels in the hierarchy or whether the focus is on open communication in all directions and across the company. However, the form of reporting and general communication will also depend on the business line and enterprise function in question so that there may well be differences even within a single bank.

### 2.8.2 Reporting

On the one hand, **internal reports** are **continuously** prepared as a function of materiality thresholds applying at different hierarchy levels. On the other hand, **ad-hoc reports**<sup>41</sup> should ensure that decision-makers can take timely measures when loss events or – within the framework of an early-warning system – risk indicators exceed certain thresholds.

A problematic aspect is that reports are frequently prepared in highly different formats and based on data from diverse sources. Overviews of reporting and regular evaluation can ensure that only the reports actually required are produced and that the reports are orientated to the information needs of the users.

As external reporting on the banks' risk management is becoming more and more important, this also applies to **external reporting** on operational risk management. Many banks include a risk report in their annual reports, be it as part of the directors' report or, in the case of IFRS reports, as a part of the notes on the annual report. The organizational units in charge as well as integration into company-wide risk management are often described in a general, introductory section of the risk reports. In most cases, the definitions used in the bank and a concise description of the most important principles and methods are provided in a section specifically focusing on operational risk management. Many banks also report on important plans and projects.

The number of major banks whose annual reports do not contain information on risks is decreasing, while there are more and more banks dedicating a separate section of their risk reports to operational risks. Today, big banks usually specify the allocation of their economic capital to individual risk categories. Only very few banks provide further quantitative information, such as the distribution of loss events across event categories.

In the framework of **reporting to banking supervisors**, reports will also have to be submitted on operational risks.<sup>42</sup> Ideally, supervisory reporting is an element of an active, open and continuous dialogue between banks and supervisors.

The **Austrian Code of Corporate Governance** constituting a voluntary self-regulation initiative of listed corporations demands in the comply-or-explain rule 66<sup>43</sup> that, in the notes to the consolidated financial statements, the company includes detailed information on possible risks, such as sectoral risk, geographic risk, interest rate risk, currency risk, risks arising from derivatives and off-balance-sheet transactions, and describes the risk management instruments applied.

The German Accounting Standard **GAS 5-10 "Risk Reporting by Financial Institutions and Financial Service Institutions"** includes, among others, rules for presenting operational risks that may also provide ori-

<sup>41</sup> To be submitted when defined risk thresholds (triggers) are reached.

<sup>42</sup> CEBS established a working group called COREP (COMmon REPorting) to ensure consistent Basel II reporting in the EU's member states.

<sup>43</sup> The Austrian Code of Corporate Governance, mainly addressing Austrian listed stock corporations, is applied on a voluntary basis. It contains the following types of rules: "legal requirement" (rule referring to mandatory legal requirements), "comply or explain" (rules to be followed, any deviation must be explained stating the reasons), and "recommendation".

entation for Austrian banks. In addition to a description of operations and legal risks, a quantitative estimate and qualitative assessment of potential consequences upon the risk's materialization, risk reports also have to cover organizational measures taken to cover and limit operational risks as well as to treat and monitor them throughout a company group.

## 2.9 Company-wide Risk Management

Control of a bank's most important risks should be embedded into a company-wide risk management system providing a **portfolio and bank-wide overview** of risks. In this context, **risk management** and an **internal control system** are complementary instruments supporting the management in achieving the objectives.

In order to establish a **common language**, to permit measurements and assessments by the same standards and to facilitate the coordinated response to risks, it is recommended to **introduce integrated frameworks** including risk management and internal control system and, therefore, the control and monitoring of risks, activities and processes throughout the enterprise. Such frameworks, be it for operational risk management or company-wide risk management, should be simple and easily understood by the addressees.

The separate management of different risks, i.e. dealing with them in isolated **risk silos**, prevents effective risk management. Risks may arise in one area and, frequently with some delay, impact other areas. But related risks may also occur in several areas and have effects across the organization whose significance is not realized in the individual areas.

Several frameworks for internal control systems and company-wide risk management are briefly presented below.

### Internal Control System: COSO, Turnbull Guidance, COCO and KonTraG

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) set a milestone in the design of internal control systems by publishing the study "Internal Control – Integrated Framework". COSO is an American committee sponsored by five organizations mainly from the fields of accounting and internal auditing. An objective of this study was to create a common language by providing a recognized definition and to establish a concept that on the basis of a broad understanding of the term "internal control", was applicable to all enterprises irrespective of their sector or size. Due to the requirements laid down for internal control systems with regard to financial reporting in the Sarbanes-Oxley Act, COSO became even more important and well-known at the international level.

The COSO concept was used by many banks as a basis of their framework for internal control systems or at least was taken into account by internal auditors in the development of risk-oriented audit approaches. In its "Framework for Internal Control Systems in Banking Organisations" (1998), the Basel Committee relies on the definitions and basic elements of internal control systems developed by COSO. In its turn, this paper was an essential basis for minimum standards and examination manuals established by banking supervisors.



According to the Basel paper, the internal control system or the internal control and monitoring system of a bank is a continuous process involving the board of directors, senior management and all levels of personnel.

The main objectives of this process are:

- efficiency and effectiveness of activities (performance objectives),
- reliability, completeness and timeliness of financial and management information (information objectives), and
- compliance with laws and regulations (compliance objectives).

This process consists of the following five interrelated elements:

- management oversight and the control culture,
- risk recognition and assessment,
- control activities and segregation of duties,
- information and communication, and
- monitoring activities and correcting deficiencies.

Chart 2.4 illustrates how the elements of this model are linked and build on each other.

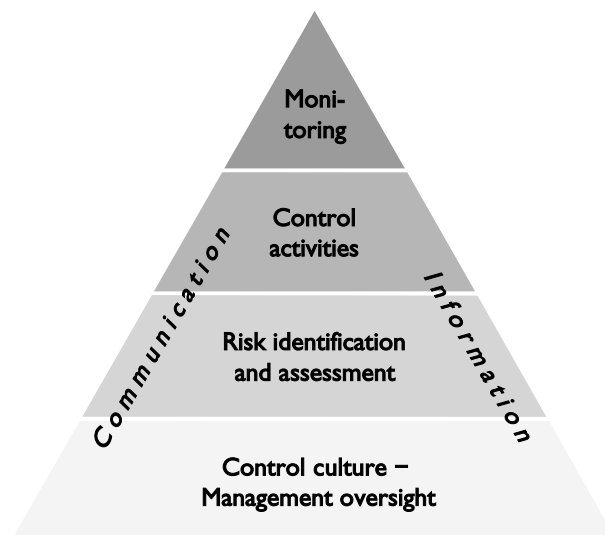


Chart 2.4: Structure and Interaction of the Elements of an Internal Control System

Two other internationally known frameworks of internal control systems are the British **Turnbull guidance**<sup>44</sup> (1999) and the Canadian **COCO** (1995). These two frameworks lean on the COSO model published a few years before them. The US Securities and Exchange Commission (SEC) explicitly lists COSO, Turnbull guidance and COCO as examples of generally accepted frameworks in its rules under Section 404 of the Sarbanes-Oxley Act.

The **Turnbull guidance** forms part of the Combined Code, i.e. the British corporate governance code. This control model contains concise, easily understandable principles for internal control systems and risk management systems which particularly stress the responsibility of the board of directors.

<sup>44</sup> Internal Control: Guidance for Directors on the Combined Code.



In Canada, the Criteria of Control Board of the Canadian Institute of Chartered Accountants issued a framework in 1995 that has become known under the name **COCO**. In its four criteria (purpose, commitment, capability, monitoring and learning), COCO stresses soft factors influencing the control environment even more than COSO.

Due to the increasing interest in risk management as well as internal control and monitoring in the wake of the **KonTraG**<sup>45</sup>, a control model was developed in Germany that has also been considered by several Austrian companies. This model is presented in the following chart.

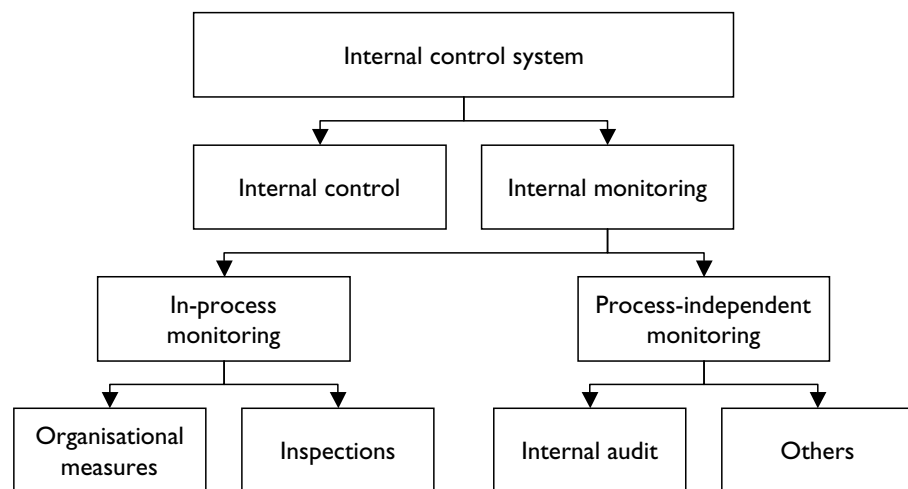


Chart 2.5: Internal Control System (source: IDW Prüfungsstandard 260 – Das interne Kontrollsystem im Rahmen der Abschlussprüfung)

### Risk Management: COSO ERM

In 2004, COSO issued a framework for company-wide risk management (“COSO ERM”) that fully integrated the internal control framework of 1992 and added several new elements. The types of objectives identified in the COSO model (performance, information and compliance objectives) were expanded by the category of strategic objectives.

The components of this model are:

- internal environment,
- objective setting,
- event identification,
- risk assessment,
- risk response,
- control activities,
- information and communication, and
- monitoring.

<sup>45</sup> The German KonTraG (Act on Control and Transparency in Business – *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich*) became effective in 1998. It (and its statement of reasons) calls for a risk management system, an internal monitoring system, including internal audit, controlling and an early-warning system.

In comparison with similar models, this framework does not contain any essentially new elements. Given its expected application by many companies, internal auditors and certified public accountants, such a model contributes to a common basic understanding and a common language.

Another risk management model, which stands out by its brief and concise nature and, in contrast to the two COSO concepts presented, also is available in a German version, is the Risk Management Standard (2002) jointly prepared by the three leading British risk management organizations IRM, AIRMIC and ALARM.<sup>46</sup>

### IT Governance

IT is a most significant area for operational risks and, at the same time, a horizontal issue touching on almost all elements of a risk management system or internal control system. IT governance models and information security management are discussed in chapter 3.2.

## 2.10 Operational Risk Management in Smaller Banks

The structure of the Austrian banking sector is characterized by numerous small and medium-sized banks. Irrespective of the regulatory approach selected, each bank faces operational risks. Even for banks opting for the basic indicator approach, it is therefore worthwhile to observe developments related to operational risk management and, where appropriate, integrate them into their own risk management approach.

When procedures for managing operational risk or risk in general are implemented, consideration has to be given to the bank's size and its type of activities. A small specialized institution active abroad, for example, has a different risk profile than a small bank with regional roots that forms part of a group fulfilling various tasks for it, such as the handling of more complex transactions.

Smaller banks especially face the problem of scarce resources, which requires a clear definition of priorities. An obvious solution is to combine operational risk management with bank-wide capital allocation – in a simple and mainly qualitative form in smaller banks. Hence, existing instruments, such as regular interdivisional meetings, should be used to take appropriate account of operational risk management. Possible further measures include meetings or workshops focusing specifically on operational risks and an examination of process documentation to see whether operational risks are adequately covered and whether there are appropriate internal controls.

External resources existing in the sector or in the bank group should be actively requested and used in the best possible way. Forums for exchanging experiences on issues such as IT help to raise awareness of potential risks and provide hints on possible measures.

Even though it is difficult to grasp and not a quantifiable element of risk management, **corporate culture** is of decisive importance for the concrete form of risk management. At present, developments in the field of risk management are strongly driven by capital markets and, especially in the case of

<sup>46</sup> Translated into German by the Federation of European Risk Management Associations (FERMA).

listed banks, characterized by a **shareholder-value** culture. In contrast, cooperative banks orientate to the task of supporting their members and aim at creating “**member value**”. What is important is that the concrete design of risk management is in line with the basic parameters of risk management, such as risk appetite, risk strategy and risk policy.<sup>47</sup>

Due to their complexity and great number of business lines, big institutions have an accordingly complicated system of responsibilities, committees, reports, etc. There, it is important to create a counterweight to formalized and hierarchically structured processes by taking account of soft, cultural factors. A smaller bank, which tends to have shorter procedures and less formalized processes, should exploit the related advantages, but not forget about a reasonable formalization and documentation of processes by means of guidelines and procedures.

If important functions, such as risk controlling, internal audit or IT operation, are contracted out, banks should be aware of the fact that **outsourcing** does not mean that the risks related to internal operation are automatically transferred to the external service providers. In part, outsourcing also involves new risks that cannot be easily recognized. These include, in particular, legal risks or the risk of a service provider failure, be it due to service interruption or economic difficulties of the partner (see chapter 2.6.3.2 “Outsourcing”). The management continues to have overall responsibility also for the functions outsourced.

One bank or the other may opt for the standardized approach at a later stage, or changes over to the standardized approach or an AMA due to a decision of the bank group to which it belongs. Such a move is greatly facilitated by early preparation.

## **2.1.1 Operational Risk Management by Securities and Investment Firms in Austria**

This chapter focuses on operational risk management by securities and investment firms subject to the regulatory requirements of the Austrian Securities Supervision Act (*Wertpapieraufsichtsgesetz*).

For investment firms, operational risk is the most important risk category because, due to their specific activities related to:

- investment advice regarding customers’ funds (Article 1 paragraph 1 item 19 lit a of the Austrian Banking Act),
- management of customer portfolios including power of disposal on behalf of the customer (Article 1 paragraph 1 item 19 lit b of the Austrian Banking Act), and
- mediation of business opportunities for the sale and purchase of one of the instruments mentioned in Article 1 paragraph 1 item 7 lit b to f of the Austrian Banking Act (Article 1 paragraph 1 item 19 lit c of the Austrian Banking Act),

investment firms are not exposed to credit risk and only to a limited extent to market risk. Thus, operational risk materializes in diverse fields and in many procedures and processes when investment firms render services. Therefore,

<sup>47</sup> See OeNB/FMA, Guidelines on “Bank-Wide Risk Management”, chapter 4.1.

investment firms also have to take suitable precautions and measures to evaluate and control operational risk in accordance with Annex V of EU Directive [2006/48/EC].

It is all the more important that investment firms know what operational risk means, where and why it may occur, how it can be identified and measured and which measures can be taken to actively manage operational risks in investment firms. In principle, operational risk is inseparably connected with almost all specific business activities, but may also arise out of the context of concrete services rendered, e.g. in the case of external events. For these reasons, the explanations on operational risk provided in chapters 1 to 3 and 4.8 of these Guidelines also constitute valuable information for identifying and assessing as well as managing and monitoring operational risks in investment firms. Hence, the term “credit institution” can basically be replaced by the term “investment firm”, bearing in mind that the proportionality principle, the scope of activities, the staff number, the customer and transaction volume, the complexity of products and processes, the organizational structure as well as the affiliation to a group have to be taken into account. In this context, special reference has to be made to chapter 2.10 discussing operational risk management in smaller banks.

In investment firms, the active management and reduction of operational risk minimizes the susceptibility to failures, while the capital charge for operational risk is to ensure that, even in the case of unforeseeable events, there is sufficient capital available to safeguard business continuity. Covering the operational risk by the firm’s capital, therefore, is an important element of comprehensive risk prevention and, thus, also forms part of strategic management.

In this context, the firm’s internal audit and external auditor play an important role in the identification, assessment, management and monitoring of operational risks in investment firms. Together with business processes defined in greater detail and a consistent internal control system, they form the basis for the identification and subsequent active management of operational risk.

For investment firms, the outsourcing of certain activities is an important issue since, due to the size of individual firms, it may well make economic sense for cost reasons to contract out ancillary activities in order to be able to concentrate on core activities in the field of financial services. Therefore, the attention of investment firms is explicitly drawn to the special characteristics and potential operational risks related to outsourcing. These are described in chapter 2.6.3 “Risk Sharing and Transfer”.

The types of operational risk and measures presented in chapter 3 of these Guidelines should provide all investment firms with valuable information and suggestions for identifying, assessing and managing operational risk. An understanding of the risks covered there and knowledge on how to deal with them also serves to create a corporate culture that allows the efficient identification of operational risks so that preventive measures can be taken to manage them. Moreover, it is important to ensure appropriate risk awareness among all employees because this generally contributes to optimizing the management of investment firms and strengthening risk culture.

## 2.12 Principles for the Sound Management of Operational Risk

In 2003, the Basel Committee on Banking Supervision published “Sound Practices for the Management and Supervision of Operational Risk”.<sup>48</sup> Key rules and recommendations for the management and supervision of operational risks are summarized in a total of ten principles.

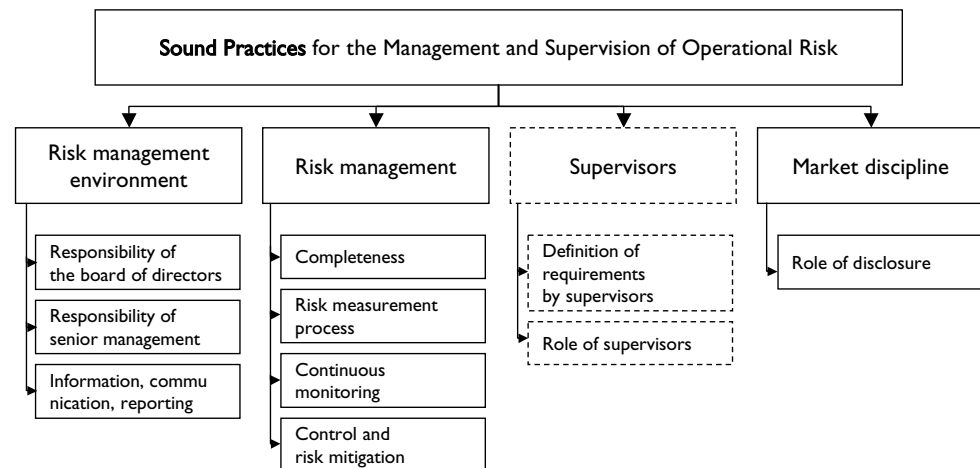


Chart 2.6: Structure of the Sound Practices for the Management and Supervision of Operational Risk

The individual principles focus on:

- developing an appropriate operational risk management environment and concrete risk management requirements,
- the role of supervisors, and
- disclosure requirements to be met by credit institutions in the context of operational risk (market discipline).

### *Developing an appropriate risk management environment*

- The board of directors should be aware of the major aspects of the bank’s operational risks as a distinct risk category that should be managed, and it should approve and periodically review the bank’s operational risk management framework. The framework should provide a firm-wide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored and controlled/mitigated.
- The board of directors should ensure that the bank’s operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff. The internal audit function should not be directly responsible for operational risk management.
- Senior management should have responsibility for implementing the operational risk management framework approved by the board of directors. The framework should be consistently implemented throughout the whole banking organization, and all levels of staff should understand their respon-

<sup>48</sup> See Basel Committee on Banking Supervision, Sound Practices for the Management and Supervision of Operational Risk, February 2003.

sibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk in all of the bank's material products, activities, processes and systems.

#### *Risk Management*

- Banks should identify and assess the operational risk inherent in all material products, activities, processes and systems. Banks should also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures.
- Banks should implement a process to regularly monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk.
- Banks should have policies, processes and procedures to control and/or mitigate material operational risks. Banks should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.
- Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

#### *Role of supervisors*

- Banking supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor and control/mitigate material operational risks as part of an overall approach to risk management.
- Supervisors should conduct, directly or indirectly, regular independent evaluation of a bank's policies, procedures and practices related to operational risks. Supervisors should ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at banks.

#### *Role of disclosure*

- Banks should make sufficient public disclosure to allow market participants to assess their approach to operational risk.

# 3 Specific Measures of Operational Risk Management

## 3.1 Systems: Infrastructure

### 3.1.1 General Risks – Infrastructure

This chapter discusses risks resulting from deficiencies in the field of infrastructure. These risks often become manifest in the wake of external events. The following chapter covers all the risks resulting from or decisively aggravated by insufficient or missing infrastructure, regardless of whether a concrete loss event has an internal or external trigger, while chapter 3.5 “External Events” explicitly focuses on external sources of risks to which companies are exposed.

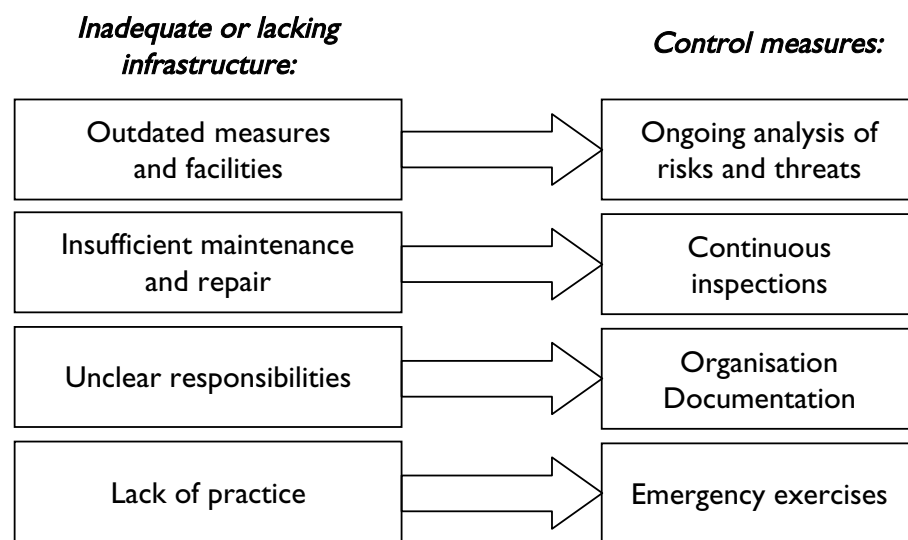


Chart 3.1: The Most Important Causes of Operational Risks in the Field of Infrastructure

Infrastructure typically becomes a risk if it is either completely missing or does not meet the requirements. The most extreme case – the complete absence of risk-relevant infrastructure in a certain field – will be hardly found in practice. But it may well be that **measures or facilities** become outdated and, therefore, no longer are adequate to provide protection against current threats. This problem that may occur in any part of the infrastructure results in the failure of actually functioning systems because they are undermined by new threats: for example, though all locks in a building are well maintained and the keys are carefully kept in safe places, this is useless if the locks in question can be easily forced open by new tools within a few minutes.

The aging of systems may constitute a serious problem (deficiencies in the field of **maintenance and repair**). While the effectiveness of certain measures, such as the structural stability or flood-safety of a data centre, does not decrease over time, other equipment needs continuous care and renewal, e.g. filling of fire extinguishers. Moreover, infrastructure that does not have a preventive purpose may become a risk factor due to inadequate maintenance (e.g. heating systems).

Risks may also arise if **unclear responsibilities** lead to mistakes in infrastructure procurement, management and/or maintenance. In this context,



special consideration has to be given to the case of fragmented responsibilities, i.e. the distribution of individual tasks and competences across diverse organizational units without one or more units having the overall responsibility. This may even result in an actual gap in security infrastructure if nobody feels responsible for a certain important part. But such poorly defined responsibilities will more frequently lead to the above-mentioned risks of outdated and inadequate maintenance.

Even optimum precautions may turn out to be ineffective if they are not submitted to **practical tests**. In emergencies, details that were forgotten in planning often give rise to dangerous weaknesses and theoretical forward-looking studies frequently neglect aspects that only turn out to be important on site and in a concrete situation. If, for example, the carefully developed alarm plan proves to be so complicated in an actual crisis situation that it cannot be implemented correctly under pressure, the crisis will be significantly aggravated. Another example that in fact occurred in practice during an exercise was that the members of the crisis team were given cell phones that, however, were not charged nor accompanied by chargers.

### 3.1.2 Special Risks – Infrastructure

As infrastructure risks can be very varied and, in their concrete form, strongly depend on the specific situation of each credit institution, a detailed discussion of individual areas of concern is not helpful, particularly since problems of security infrastructure have long been known and studied in detail in the banking sector. Therefore, only a few areas are outlined below that need to be especially emphasized in the context of operational risk (many of them belong to the oldest security problems in banking).

- Problems of **unauthorized access**. Protection has to be ensured not only for assets, but nowadays also more and more for frequently sensitive information; this applies to practically all business premises. Please note that unauthorized access may not be limited to cases where force is used, but may also be obtained, for example, by deceit. In addition to entry by external persons, cases also have to be considered in which employees try to get access to areas that – for whatever reason – should be reserved for a limited number of persons.
- Problems related to the **safekeeping and transport of assets**. Such risks may be considerably increased by deficiencies in security infrastructure – in line with the old saying that “opportunity makes the thief”. Hazards occurring in this field include robbery (typically an external event), larceny (internal or external) or embezzlement (internal).
- Problems caused by the **elements**. These are external events, which are discussed in greater detail in chapter 3.5. In this context, it should only be pointed out that a certain minimum of effective precaution against such risks is indispensable because otherwise even minor incidents may result in major damage. For example, a fire in a wastepaper basket that can be rapidly discovered by smoke detectors and immediately extinguished with fire extinguishers available on site could develop into a serious loss event without such protective equipment. This applies particularly to building parts housing sensitive functions, such as data centres (see below).

- Problems related to **power supply**. The increasing reliance on technologies in banking, especially the dependence of numerous processes on IT systems, results in an elevated vulnerability to an interruption of power supply. In addition to blackouts in the region where a credit institution is located (again a typical external event), the cause of interruption may also be found inside a bank (electrical shorts and similar incidents). Potential consequences of interrupted power supply are not limited to problems related to IT systems (data loss, possible damage to equipment), but may be much more complex: stalled elevators, non-working communications equipment such as phone and fax or the absence of lighting alone severely disrupt business, especially if power supply is interrupted for a longer period of time.
- Problems related to the **telecommunication service** provider. Critical service areas are not only fixed and mobile telephony as well as fax communications, but also data lines inside a company and to the outside world. A standstill of the internal network may well have severe adverse effects on a credit institution's core processes since the connection to the server is interrupted so that a database or a key application is not available. The concrete impact of this risk rises as the dependence of a specific business line or process on the telecommunications service concerned increases and as the number of options for using other communication media instead of the failed system decreases.
- Problems related to the **availability of information technology**. Critical factors not only result from power supply or network failures, but may have numerous other causes:
  - application or server failures,
  - diverse hardware defects,
  - disruptions caused by hackers or malware (see the explanations in chapter 3.2), etc.

Depending on the extent of IT support required in a business process, the effects may range from minor delays in processing to a complete standstill in one or more business areas so that inadequate preventive measures taken in this field may significantly raise the risk level of a credit institution.

- Problems due to **data loss** (e.g. customer data, items entered, buy and sell orders or account balances). While business may already be considerably impaired if access to data is not possible for a limited period of time only, damage to data or their destruction may even threaten the existence of a bank in extreme cases. As a result, lacking precautions in this field also constitute a significant operational risk.

A common characteristic of all the risk areas identified is that the risk level varies depending on the environment and business line. In practice, it will not be possible to cover all risk factors possible across all fields of a credit institution with reasonable efforts so that risk awareness is of special importance with a view to identifying the relevant risks. Thereby, excessive efforts can be avoided that are not paralleled by relevant potential exposures. All the more important it is, however, to give more attention to those fields in which vulnerability is particularly high. While, for example, a legal division is not likely to be strongly dependant on the permanent availability of telecommunication

services and IT systems, the situation will certainly be different in the case of securities trading.

### 3.1.3 General Measures – Infrastructure

The information presented above clearly shows that an **analysis of risks and threats** is the most important starting point for all further measures in the infrastructure field. Such an analysis – carried out within the framework of a general risk analysis, in the form of special needs assessments for specific risk types and areas as well as in the form of a continuous evaluation and adaptation process – is the only means to ensure that the necessary measures can be taken and adjusted as required. Depending on the size of the credit institution and the scope of its business activities, a suitable procedure is to be defined in order to obtain an adequate evaluation of the relevant risks and to assess the individual business lines, sites and resources with regard to their exposure and importance for business operations (see also chapter 2.5 “Risk Identification and Assessment”).

The next basic set of measures relates to the infrastructure’s **organization, management and documentation**. Questions to be answered in this context are, for example:

- **How are responsibilities assigned within the enterprise?** If competences are highly dispersed, coordination measures (coordination bodies, security platforms, staff units with coordinating functions, etc.) may be particularly needed in order to permit an integrated overview and to prevent that responsibility gaps give rise to risks.
- **Are there clear procedures for maintaining and renewing infrastructure?** This is especially important for security infrastructure to ensure that, on the one hand, new threats can be coped with adequately and, on the other hand, existing facilities do not lose their effectiveness due to inadequate maintenance. Even infrastructure that is not intended to mitigate risks can become a risk itself (e.g. loose roof tiles that could injure passers-by or lead to rainwater damage).
- **Are the resources and knowledge required available?** In addition to providing the necessary material resources, the enterprise also has to make sure that adequately trained employees are available (e.g. fire protection officers, security officers, etc.). In this context it is important that know-how is continually kept up to date, i.e. training should not be limited to a single course but provided on an ongoing basis.
- **Is infrastructure well documented in all important areas?** Just as an emergency power supply can hardly be planned without a cabling plan, the preparation of evacuation plans requires information on the location of emergency exits; IT security concepts cannot be drawn up without an inventory of IT infrastructure. Measures should be taken to ensure that the documentation is regularly updated and accessible in a suitable form. It is to be borne in mind, however, that while this documentation contains sensitive information that has to be adequately protected, reliable access to a part of this information has to be ensured especially in emergencies.

Finally, the **careful, continuous review** of the infrastructure is a necessary measure to prevent that risks from these sources arise or increase. This is not

limited to a regular inspection of the status of facilities and systems that has to form part of the above-mentioned maintenance activities, but also has to include special checks taking account of the relevant circumstances and risks. In addition to elevated general attention in those fields in which the analysis of risks and threats identified a higher need for protective measures, it is particularly important in this context to organize exercises applying the emergency measures and plans defined. Such exercises should take place at regular intervals to evaluate the measures taken and, at the same time, develop a certain routine facilitating controlled action in emergencies.

For some risks, it makes sense to practice behaviour in emergencies, e.g. in the form of fire protection and evacuation exercises. This category also includes failure tests for mainframe systems, practicing the switch to secondary data centres and similar exercises. The results should be fully documented in order to record difficulties encountered as well as weaknesses and possible improvements identified. This can also ensure that the experiences made are input into an improvement process.

Throughout this field, it is also necessary to comply with the applicable legal regulations and conditions specified by authorities (e.g. in operation permits) that define certain measures of risk prevention as well as regular inspections. Examples are fire prevention regulations contained in the Land fire authority acts with their provisions on the inspection of fire protection installations.<sup>49</sup> Any violation of such regulations not only gives rise to a dangerous risk potential, but also involves the risk of losses due to non-compliance with legal obligations, i.e. a legal risk (see chapter 3.6).

#### 3.1.4 Special Measures – Infrastructure

The explanations provided in chapter 3.1.2 also apply to the special measures taken to limit infrastructure risks: the great variety of possible areas and highly different circumstances require that each credit institution takes its own specific measures whose extent and level of detail depends on the results of the analysis of risks and threats. Therefore, only a few areas are to be highlighted as examples below.

**Adequate access restrictions and security measures related to the safekeeping of assets** have long formed part of the core tasks in the security organization of credit institutions so that they need not be discussed in detail here. In this field, too, the above statements naturally apply with regard to organization, management and documentation.

**Damage caused by the elements** includes, on the one hand, risks that are virtually independent of the location of a credit institution, such as damage caused by fire, lightning or water. For these general risks, appropriate measures have to be taken anyway since building regulations, fire protection provisions, etc., specify certain minimum standards. In addition, however, consideration has to be given to the fact whether the results of risk analysis point out further hazards requiring special measures. For example, certain installations – especially in the IT field, such as data centres, telephone junction boxes, etc.

<sup>49</sup> In Vienna, for example, the Viennese Fire Authority and Clean Air Act (*Gesetz über die Feuerpolizei und Luftreinhaltung in Wien*), Land Law Gazette 1957/17, as amended.

– are particularly vulnerable to water exposure. This has to be born in mind not only when planning fire extinguishing systems, but also may significantly increase the severity of damage from a burst water pipe.

Other special sources of hazards may result from the geographic location of a site. In flood-prone areas, specific precautions need to be taken, especially with regard to particularly sensitive installations. Here, it also might be necessary to take account of any vulnerability to power supply fluctuations. Furthermore, especially sites abroad can be exposed to distinctly different risks both with regard to potential structural weaknesses in power supply or telecommunication services and the range of possible damage caused by the elements (earthquake zones, hurricane areas, etc.). Such risks require the preparation of special disaster plans and specific protection measures in the infrastructure field.

Due to the strong dependence of numerous processes on well-functioning IT systems, **IT infrastructure** is of great importance. Here, a package of various measures is necessary with regard to **business contingency planning** to adequately respond to the risk of system failures and data losses especially in the following fields:

- **Measures defined in business continuity planning (BCP)** are to ensure that the failure of an IT system can be bridged by backup and temporary solutions. For this purpose, critical systems need to be managed with redundancies with the following variants being possible:<sup>50</sup>
  - Backup systems are taken into operation when necessary; this is the simplest, but also the slowest solution.
  - Several systems work together in a cluster so that they can replace each other if one of them fails.
  - In fully failure-tolerant systems, all the components are characterized by redundancies and, hence, particularly well protected against failures.

The variant selected depends on the importance of the systems used in the overall context of the IT infrastructure and has to be assessed for each part of the IT environment of the credit institution in the risk analysis. The solution actually implemented has to be tested regularly. If parts of IT systems or the entire IT infrastructure of the credit institution is outsourced, this fact also has to be separately considered when designing these measures (see also chapter 2.6.3.2 “Outsourcing”).

- **Disaster recovery (DR) measures** go one step further by aiming at maintaining emergency operations when major parts of existing systems are destroyed, e.g. in a natural disaster. Depending on the volume and complexity of business activities and IT systems used, various solutions are possible, such as:
  - Contractual arrangements with an IT service provider on the provision of backup equipment when needed is a relatively simple option, but requires specific measures to ensure that data and application software can be transferred to the backup systems. Moreover, this procedure is relatively time-consuming in an emergency, which has to be taken into

<sup>50</sup> Verstaen, Business Continuity, 2003.

account in plans. At any rate, the contract should specify how fast backup solutions need to be made available in emergencies; consideration also has to be given to the fact that such arrangements may give rise to risks typical of outsourcing solutions (see chapter 2.6.3.2 “Outsourcing”).

- The use of the company’s own test systems as a fallback solution is a possible alternative especially if these systems have the required capacity; moreover, test and production environment should be physically separate to prevent the risk of losing both systems due to the same loss event at the same time.
- The establishment of a separate backup data centre – by the credit institution itself or an IT service provider – is the most expensive, but also most secure solution. Apart from a backup data centre that is only activated in the event of a crisis (the issue of data transfer has to borne in mind in this case, too), it is also possible to have two data centres working in parallel operation so that when one centre fails, the other one can automatically take over the entire workload. This also means that all the data are stored twice so that this particularly resource-intensive variant can also ensure a relatively short delay until the systems are available again.

Regardless of the nature of the measures taken, the concrete procedure for switching to fallback systems should be planned in detail, documented and regularly exercised (see chapter 3.1.3 “General Measures – Infrastructure”) in order to check whether the procedure is feasible in practice and how long it takes until at least emergency operations can be resumed. Credit institutions not operating their IT systems themselves, but using an IT service provider or a joint data centre should ensure that their partner takes the required measures for maintaining business operations and regularly tests them.

- The issue of **uninterruptible power supply (UPS)** also falls under the heading of BCP and DR measures. Critical systems have to be protected by suitable equipment against power failures and power supply fluctuations. Just like all parts of security infrastructure, this equipment also has to be regularly maintained and inspected.
- **Backups of enterprise data**, finally, are an issue of special importance since large parts of banking activities rely on the availability of diverse data due to the increasing use of technology. Therefore, suitable measures must be taken to minimize the risk of partial or full data loss by planning the data backup process in detail and supporting it with the required technical resources. The procedure (way of data backup, systems and storage media involved, responsibilities, regular checks of the systems as well as the data backed up) have to be laid down in a backup policy. The way in which backed-up data are stored should contribute to mitigating risks (safe storage, physical separation from production systems, etc.).
- IT systems, data centres, stores for backup copies and similar facilities are, of course, also typical areas to be protected by **more stringent access controls** and **physical security measures**. Their elevated vulnerability to certain natural hazards also has to be adequately considered.



Infrastructure risks also can be controlled by insurances to a certain extent. Insurance products covering physical damage to installations have long formed part of the standard offering of the insurance sector. There are, however, also special insurance products for the risks specific to IT infrastructure (e.g. business interruption insurance). Please note that, especially in the latter case, it may be necessary to prove a concrete loss – and especially the concrete amount lost – in order to be able to receive insurance payments.

## 3.2 Systems: Information Technology

### 3.2.1 General Risks – Information Technology

The more and more intensive IT support of all enterprise activities facilitates processing, especially in retail business, but also results in special operational risks. In contrast to the risk sources discussed in chapter 3.1, the hazards covered here rather relate to “intangible” fields, such as software and organization. Therefore, the following main risks are to be mentioned:

- **Inadequate software quality** gives rise to a broad range of dangers. This area relates not only to defective customized software, but also to off-the-shelf products that may cause quite similar loss events due to errors by the producer, compatibility problems or mistakes made in software configuration. The most serious problems are complete system crashes that can cause considerable losses not only due to lost data, but also due to the delay until the system is functional again. Processing errors may be equally dangerous as they might not be detected right from the start and only trigger high correction efforts later on. Even a system that basically works without any errors may harbour risks due to excessive processing times or high resource consumption (computing time, network performance, etc.). In addition to those defects that directly impact IT systems and, therefore, can be assigned to this risk category without any problems, consideration also has to be given to the error potential indirectly caused by defective IT systems in other areas. A cumbersome data input template, for example, may increase the risk of user errors (a defective system leads to mistakes made by employees); inadequately implemented security measures facilitate criminal acts (risks of internal or external fraud). Likewise, an IT system that rather impairs than supports a process may raise process risk. While losses triggered by such risks are typically assigned to the relevant direct event categories (internal/external fraud, settlement, delivery and process management, etc.), it makes sense in these cases that risk prevention focuses on the upstream cause, i.e. information technology.
- **IT security** is a particularly important, separate risk area. In addition to the security issues already dealt with in the context of infrastructure (see chapter 3.1), the following main topics have to be addressed:
  - Unauthorized access by third parties**, be it to spy out data, to make personal gain, to commit an act of sabotage or to use the credit institution’s resources for one’s own purposes.
  - Unauthorized access by employees** of the credit institution. Such incidents are primarily attributed to staff risk, but they also have to be



addressed by preventive measures in the area of IT systems and IT organization.

**Malicious software** (or “malware” for short) **designed to cause damage**; it includes viruses (spread by attaching to other files and infecting them), worms (propagate through networks by infecting other computers), Trojan Horses (conceal their real purpose of causing damage by claiming to be a harmless program in order to be installed by the user), etc. While some of these programs cause damage, at worst, by consuming resources for spreading themselves, there are also cases in which data are deleted, manipulated or transferred to third parties, system crashes are triggered or programs are installed on the infected computers allowing hackers to access the system through a “backdoor”.

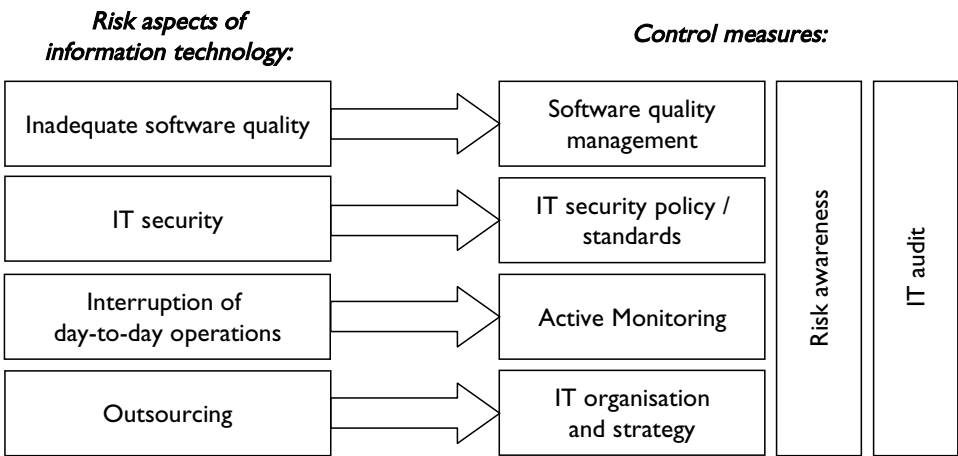


Chart 3.2: Some Aspects of Operational Risk in Information Technology

All these risks can dramatically increase in importance due to **deficiencies in the security policy** of a credit institution. For example, careless handling of passwords or inappropriate administration of access rights not only facilitates the “work” of external attackers, but also the internal potential for misuse strongly rises as the opportunities for unauthorized access increase due to security gaps (all the more since the company’s employees frequently know about deficiencies in security organization and, thus, are able to exploit them). The hazard resulting from malware is also considerably higher in the absence of appropriate protective measures because numerous viruses and worms are detected and eliminated by up-to-date protective software without any problems, but constitute a serious threat when outdated or no anti-virus systems are used.

**3.2.2 Special Risks – Information Technology**

Apart from the importance of information technology and the related risks for the entire enterprise, separate consideration has to be given to areas in which IT-related risks take on a specific form or are of special significance. If IT risks are addressed only at an excessively global level without targeting particularly important or exposed areas, this perhaps results in a certain basic security, but may be insufficient especially in areas where it would really matter.

It has already long been impossible to handle the heavily automated **processes of retail business** at the required speed and efficiency without modern computer systems. It is all the more important to focus on the prevention of risks, ranging from a failure of the systems used, the problem of possible data loss and data abuse to damage caused by defective or inadequate IT systems. In some cases, the reliance of such processes on functioning IT systems may be addressed by going back to manual processing in emergencies; but such scenarios require adequate planning and regulation in advance so that manual temporary solutions need not be improvised in crises, which could cause even higher losses.

Apart from these processes, there are **particularly sensitive business areas** that require elevated attention, e.g. securities and foreign exchange trading in which records held in IT systems regularly represent high values. In all business lines where IT is used to manage or transfer high amounts, the risk of abuse is particularly high. The fact that trading transactions are extremely time-critical also justifies higher security measures for this business line (mainly with regard to system stability and software quality) because any disruption of business can lead to high losses. The identification of such sensitive business lines, which will differ as a function of the credit institution's activities, therefore, is an essential requirement for planning adequate security measures.

**Data protection** is an issue that needs to be addressed separately, not least due to specific legislation in this field. The provisions of the Data Protection Act<sup>51</sup> have to be complied with not only due to the legal consequences foreseen (imprisonment or administrative fine), but also because the insufficient protection of sensitive information increases the risk of intentional abuse or careless handling of such data. The resulting damage may materialize in diverse areas and ranges from labour disputes and damages claimed by customers to the enforcement of the rights to information, rectification and deletion of data; possible reputation damage that would be caused, in particular, by the careless handling of customer data usually does not fall under the definition of operational risk, but can well have a significant impact in practice. In this context, it is to be borne in mind that data protection is not limited to information held in IT systems. Paper-based information, too, is covered by the same data protection legislation and has to be handled accordingly.

The risk situation is complex in cases where information processing has been **outsourced** in part or even in full to one or more third companies. Due to the growing trend to contract out considerable parts to subsidiaries or third-party providers especially in the IT field, this issue is of particular importance (see also the general explanations in chapter 2.6.3.2 "Outsourcing"):

- The **business partner risk**, which can reach major proportions due to the high IT dependence of numerous processes, has to be considered right from the start and minimized by appropriate measures. A failure of the outsource provider not only involves the risk of business interruption due to the unavailability of critical systems, but also the risk of data losses.

<sup>51</sup> Bundesgesetz über den Schutz personenbezogener Daten, Federal Law Gazette I No. 165/1999, as amended.

- The **legal risk** that may arise from fuzzy provisions on the duties of the outsource provider has to be considered primarily with regard to availability, minimum response times in the case of problems and the provision of standby capacity.
- If adequate control, information and auditing rights are not given to the credit institution beforehand, there is also a **risk of losing control of core processes**.
- A hazard that must not be neglected especially in the IT field is the **loss of know-how**. Given the rapid development of IT, the transfer of key parts of technical competence may lead to a very high increase of the dependence on the outsource provider, which also makes it difficult to plan any exit strategies.

In the field of **overlap between IT risk and other risk categories**, there are two more issues to be considered: On the one hand, switches from computer-assisted to manual processing and vice versa constitute a potential weakness in business processes that has to be addressed by suitable means (see the explanations on media changes in chapter 3.3); on the other hand, it is particularly in the IT field that there are often employees with highly specialized know-how and skills whose unavailability (due to termination of employment or longer sickness leave) results in a dangerous bottleneck in the IT organization (see the explanations on key personnel in chapter 3.4).

### 3.2.3 General Measures – Information Technology

In the IT field, comprehensive measures are possible and necessary to limit the risks identified above in a suitable fashion. In fact, these are packages of measures which are presented in an overview below; their concrete scope and detailed implementation strongly depends on the size of the credit institution, the complexity of the IT systems used and the influence of information technology on business processes.

A basic framework for the consideration of these topics is already defined by the **organization of the IT field**. In this context, the following questions have to be answered:

- **How big is this area?** Especially in credit institutions with numerous self-developed applications, a high number of employees deals with IT issues. It has to be ensured that the organizational structure is appropriate to the scope of tasks – from a single IT division to a separate subsidiary in charge of software development, application support and operation of the data centre.
- **Who is responsible for IT security?** There are several options each having its pros and cons. Setting up a security team within the IT division permits a strong involvement of the persons responsible for security in day-to-day IT operations and facilitates communication, while responsibility for IT security outside the IT field (e.g. the organizational unit in charge of all security measures from structural to IT security) offers the advantage of more effective control due to this segregation of responsibility (IT and IT security may even be assigned to different members of the board of directors) and facilitates the development of a comprehensive security concept by summarizing all security aspects. At any rate, clear responsibilities and

the related competences are required to avoid that IT security is considered to be a marginal issue.

- **Does the IT field have the required resources?** This question does not relate exclusively to material resources; in particular, qualified personnel may constitute a special bottleneck. In addition to mere capacity planning, consideration also has to be given to the availability of the required expertise and skills because specialized IT knowledge has a particularly short “half-life”.

The more fundamental issue of the **credit institution’s IT strategy** is closely linked to IT organization. In the absence of such a strategy, the IT systems of a company will soon become an unsystematic patchwork of components acquired to solve specific problems or to cover current needs without pursuing a homogeneous policy. To prevent such a situation, there should be clear specifications at a strategic level defining the framework and also outlining future steps. At the board level, there should be a clearly defined responsibility for the IT systems of the credit institution.

The IT strategy serves as a basis for planning the entire IT area; it should contain explanations on infrastructure (sites, hardware, structural security measures, emergency facilities), software (operating systems, self-developed or third-party applications, criteria for selecting systems) and personnel (deployment of employees, education and training) and define the framework for the company’s security policy. Considerations on outsourcing should also be integrated into the general IT strategy.<sup>52</sup>

**Prioritization** is recommendable as a part of the IT strategy and to make it more specific. By identifying the core applications and processes with IT support it is possible to assess the need for security measures, contingency plans and similar measures in a targeted manner, which facilitates the use of resources for risk-mitigating measures where they yield the biggest benefit.

The problem of inadequate software quality is to be addressed by suitable **software quality management**. This complex field, whose required scope strongly depends on the complexity of the systems used and the volume of self-developed software, includes, for example, the following issues:

- Especially in the case of self-developed software, **testing** is of great importance. Application development of more than just minor proportions<sup>53</sup> always requires a clearly defined test strategy, including several levels of systematic tests. For each development project, a test concept or test plans have to be drawn up in line with that strategy. The test cases planned as well as the results of the tests should be documented in sufficient detail so that an outside expert can get an overview of the scope and depth of testing. In addition to foreseeing sufficient time and human resources for tests, technical infrastructure (test environment separate from production, test data) also has to be provided. While software tests are particularly important for self-developed systems, off-the-shelf software must also undergo testing before being put to real operation, even though the main focus in

<sup>52</sup> See Kreische, Anforderungen an die Informationstechnologie, 2003.

<sup>53</sup> When an Excel sheet with currency conversion functions is prepared, there is, of course, no need for a multi-step test.

this case is on content requirements and the interoperability with other IT systems.

- **Software quality assurance as a whole** goes beyond merely testing systems. As the cost of error correction is lower if errors are detected as early as possible in software development, it makes sense to take appropriate quality assurance measures already during analysis and design phases. Examples of such measures are the early involvement of the user division in the development process, the systematic preparation of comprehensive and binding specifications, the establishment of test plans and test cases already during the initial project phases, etc. Mutual quality controls (code reviews) during development, too, fall in this category.
- **Mandatory version and configuration management** that is as comprehensive as possible ensures that control of the systems used and their current components is not lost and prevents numerous problems that may arise from version conflicts and the like. Depending on the complexity of IT systems, the options range from manual lists and organizational rules to computer-supported solutions.
- **Clear and well-documented processes** must be established for software quality management to regulate competences, responsibilities and procedures. Examples for such arrangements are development guidelines, rules for transferring software to the production environment, project manuals, sample specifications, etc.

To achieve an appropriate level of protection in the field of IT security, a comprehensive enterprise **IT security policy** needs to be adopted that lists all the measures to be taken in the context of IT-related security precautions. In the absence of such a policy, there is a risk that individual security measures are taken, but, due to a lacking overview, security gaps emerge in fields not covered by individual measures. Moreover the security policy constitutes a binding catalogue of instructions on IT security for all employees of the credit institution and, thus, is an important instrument in staff training (see the information on awareness programs below).

Like all documents of this type, the security policy has to be adjusted to the complexity of the field in question with regard to the depth and level of detail of its rules. Above all, it has to be borne in mind that excessively detailed rules are not only more difficult to update, but also run the risk of being neglected or circumvented in practice. What is more important than detailed descriptions of individual work steps and measures – which are better discussed in separate work instructions for the unit in charge – is to establish guidelines covering, if possible, all aspects of the subject, while treating them at a relatively general level and complementing them by separate documents on specific issues. The guidelines should mainly discuss the following areas:<sup>54</sup>

- Information security objectives and strategy (bearing in mind that both are to be in line with the corporate strategy);
- Organizational structure (responsibilities and competences) of the security field;

<sup>54</sup> See Österreichisches IT-Sicherheitshandbuch, 2004.

- Risk analysis strategies (including reflections on the acceptable residual risk);
- Classification of data available in the company by their need for protection with regard to confidentiality, integrity and availability taking into account that data managed on paper and not in IT systems also has to be covered (general questions of information security). Considerations on data protection also fall into this field;
- Classification of IT applications and systems by their importance for day-to-day business, misuse potential, etc. (building on the prioritization mentioned above); and finally
- Activities for reviewing and maintaining security.

The framework conditions for central protective measures (fundamental reflections on firewalls and anti-virus systems as well as measures to raise awareness) and the basic design of measures to maintain business operations (see the explanations on business continuity management in chapter 3.1.4 “Special Measures – Infrastructure”) should also be outlined in the security policy. To avoid gaps in the overall concept arising from the focus on IT systems, it is worth considering whether the policy should cover information security as a whole (in contrast to IT security alone) in order to include also hard-copy documents, for example, which may also contain confidential information and be necessary for functioning business processes, in a single security concept coordinated with the technical partners.

At any rate, it is to be borne in mind that the preparation and adoption of a security policy requires much work and is by no means a one-time process. By necessity, the security policy also includes processes ensuring that the guidelines are continuously reviewed and adjusted to changing requirements and to the technical situation. An adequate security level can only be guaranteed by a “living” overall concept adjusted to practical operations, while a security policy prepared as a mere “paper exercise” for documentation purposes may even create the dangerous illusion that all the measures necessary have been taken anyway (pseudo-security).

For the **ongoing operation of IT systems**, measures have to ensure on the one hand that operation is appropriately monitored in order to detect and respond quickly to failures as well as security-relevant events; on the other hand, procedures have to be established to make sure that the measures taken in the enterprise to limit IT risks are continuously adjusted to the changing environment. As a result, the following topics need to be addressed:

- **Trouble-shooting processes** ensuring that solutions for technical questions and problems are offered to users of IT systems within an adequate period of time (depending on the criticality of the business processes or applications in question). Rules should exist not only for eliminating malfunctions, but also for documenting them because, in the case of recurring problems, the existing solution can be applied more quickly and the identification of patterns can make it easier to study the causes of problems.
- Since apparent “system problems” may also be signs of security-relevant incidents, it should be ensured that trouble-shooting processes and **processes for dealing with security-relevant incidents** are not completely independent of each other. This may be achieved by creating an



interface between the help desk and the security division which, however, requires that the help-desk staff has sufficient knowledge for realizing whether a supposed malfunction could be a symptom of a security problem (e.g. system crash due to virus infection; decline of network performance due to a Trojan Horse, etc.).

- Additionally, **ongoing operation has to be actively monitored**, which may be done in different ways depending on the complexity and importance of the IT systems. Options in this field are the monitoring of processes, servers and similar components by administrators, automatic system monitoring and diagnostic tools and intrusion detection systems automatically looking for “suspicious” activities within a network. Especially in sensitive areas, suitable logging measures need to be taken to facilitate the detection and investigation of unauthorized access cases (appropriate log files, etc.). It is to be ensured, however, that the borderline to unlawful employee surveillance is not crossed; in case of doubt, the works council has to be consulted in advance.
- In this context, the maintenance of ongoing operations in a broader sense also includes **processes for updating systems and security measures**. In particular, there should be continuous processes for regularly and frequently supplying the anti-virus system with up-to-date malware data, maintaining systems such as the firewall or the intrusion detection system (closing security gaps, optimizing configurations) as well as updating other critical systems (loading of patches and security updates of operating systems as well as standard software used). Moreover, there should also be rules with regard to the frequency, competence, performance and documentation of this work. Checks on whether these updating processes are actually carried out are important measures for reducing risks in this field.

Raising **risk awareness** is one of the most important contributions to minimizing risk in general. This particularly applies to IT risks since there is a wide-spread, but wrong impression that this issue was exclusively relevant to the staff of the IT division (or security division if responsible in organizational terms). In fact, IT security is of concern to all employees because the biggest security gaps frequently are caused by human and not technical factors – in particular in systems of high technical security level. Careless handling of passwords, installation of software without prior checks, opening seemingly harmless e-mail attachments – all those are examples of risks that relate to the IT field, but can just as well be considered as aspects of staff risk. Promoting greater awareness of risks linked to information technology, therefore, needs to be an essential part of a credit institution’s overall security policy. Appropriate **awareness-raising measures** are, for example, the clear and comprehensive communication of the IT security policy, training on the most important IT-relevant threats in day-to-day business, promoting a feeling of how important it is to safely handle passwords and similar access data; risk awareness checks may also be performed.

Finally, a comprehensive, general measure to mitigate IT risks is the introduction of **standards on IT security and/or quality control**. In the security field, noteworthy standards primarily are the international standard



ISO 17799:2000<sup>55</sup> or the British standard BS 7799<sup>56</sup>, which formed the basis of ISO 17799, as well as ISO 13335:2000 (made up of five documents covering different aspects of IT security). In addition, the IT Baseline Protection Manual issued by the German Federal Office for Information Security<sup>57</sup> gives an overview of threats and fundamental security measures, which, however, have to be supplemented by further measures in particularly sensitive areas. The IT Baseline Protection Manual also formed an important basis for the Austrian IT security manual (Österreichisches Sicherheitshandbuch) that the Secure Information Technology Center – Austria (A-SIT)<sup>58</sup> revised in 2003 and updated in 2004 on commission by the Federal Staff Unit for ICT Strategy<sup>59</sup>. This manual is now also available in the XML format<sup>60</sup>. Such manuals constitute a useful starting point when security guidelines are drawn up to make sure that all aspects are covered and an integral picture is obtained of the requirements that the security policy of the credit institution has to meet.

*BS 7799 is a British standard laying down the specifications for information security management systems (ISMSs). It mainly deals with the establishment of IT security management and its integration into an organization. The standard does not contain detailed information on implementation, but defines horizontal requirements. By information security, BS 7799 understands the maintenance of confidentiality, integrity and availability of information.*

*BS 7799 is made up of two parts:*

- *a “Code of Practice for Information Security Management” identifying controls that are essential for information security management<sup>61</sup>, and*
- *“Specifications for Information Security Management Systems” including a framework for information security management and, in analogy with the quality management standard ISO 9000, a plan-do-check-act cycle, i.e. a process-oriented approach for implementing an ISMS.*

*The first part of this standard was adopted as the international standard ISO/IEC 17799 containing best-practice recommendations for information security management. In 2003, these standards have been incorporated into the Austrian body of standards as ÖNORM ISO/IEC 17799 “Informationstechnologie – Leitfaden für das Management der Informationssicherheit” and ÖNORM A 7799 “Informationssicherheits-Managementsysteme – Spezifikation und Hinweise zur Nutzung”.*

*Certification according to BS 7799 or ISO/IEC 17799 frequently forms part of contracts on the outsourcing of critical IT processes. The implementation of such a model may, however, also support information security, for example, with regard to information relevant to risk management, such as loss event data from the field of operational risk.*

Examples of comprehensive IT standards that also cover aspects of IT security are the **COBIT** (Control Objectives for Information and related Technol-

<sup>55</sup> In Austria available as ÖNORM ISO/IEC 17799 from the Austrian Standards Institute.

<sup>56</sup> In Austria available as ÖNORM A 7799 from the Austrian Standards Institute.

<sup>57</sup> The manual can be downloaded free of charge from <http://www.bsi.de>

<sup>58</sup> <http://www.a-sit.at>

<sup>59</sup> <http://www.cio.gv.at>

<sup>60</sup> <http://www.cio.gv.at/securenetworks/sihb/>

<sup>61</sup> Information security policy, security organization, information asset classification and the control of those assets, personnel security, physical and environmental security, communications and operations management, access control, systems development and maintenance, business continuity management and compliance. These issues are to be covered by internal guidelines and examined, for example, in IT audits.

ogy) standard prepared by ISACA<sup>62</sup>, the professional organization of IT auditors, as well as the IT Infrastructure Library (ITIL) of the British Office of Government Commerce<sup>63</sup>. If properly implemented, such systematic approaches for improving IT quality and security can contribute to reducing risks from safety deficiencies and inadequate software quality.

*COBIT is an internationally recognized standard for assessing and auditing the IT governance of enterprises. It mainly focuses on IT security and quality assurance of IT processes. Numerous other standards are taken into account, including COSO and ISO 9000. In the IT process cycle, COBIT differentiates between the following domains:*

- *planning and organization,*
- *acquisition and implementation,*
- *operation and maintenance,*
- *monitoring, and*
- *information.*

*In these domains, a total of 34 IT processes are distinguished. Criteria for analyzing them are critical success factors, key goal indicators and key performance indicators.*

*COBIT is used by the IT auditors of a number of banks. In operational risk management, this model may be used to prepare a risk and control self-assessment to study IT aspects in a business process analysis and to develop risk indicators.*

It is, however, true for all standards and frameworks that they do not serve their purpose if they are implemented as an end in themselves instead of being filled with life and integrated into a company's actual processes (see also chapter 3.3.2 for general quality standards in process organization).

#### 3.2.4 Special Measures – Information Technology

Since specific **insurance products** have been available for the IT field for a long time, it makes sense to look deeper into this special form of risk prevention. In addition to business interruption and property insurance (see chapter 3.1 “Systems: Infrastructure”) that is important in the infrastructure field, products offered include computer abuse insurance (against damage caused by internal IT-related crime) and software insurance (against damage to programs and/or data caused by force majeure, user mistakes or intent). Legal expenses and liability insurances also cover special parts of IT-related risks (e.g. liability for breaches of data protection legislation).<sup>64</sup>

Some aspects, however, must be borne in mind: As a rule, such insurances only cover quite specific types of damage with narrow definitions. Full insurance coverage against all types of IT risk, therefore, will not exist in most cases. Moreover, insurance companies, as a rule, reject claims in cases in which the insured party failed to take measures limiting or preventing damage. If, for example, an enterprise does not regularly update its anti-virus system, the insurance company could refuse to pay or at least delay payment in a lengthy legal dispute. Just like in other fields, insurances cannot replace risk-limiting measures.

<sup>62</sup> Information Systems Audit and Control Association, <http://www.isaca.org>

<sup>63</sup> <http://www.ogc.gov.uk>

<sup>64</sup> Romeike, IT-Risiken und Grenzen traditioneller Risikofinanzierungsprodukte, 2000.

In the case of IT **outsourcing**, too, the credit institution has to make sure that it stays in a position to assess the risk situation and take appropriate measures to limit risk (see also the general explanations in chapter 2.6.3.2 “Outsourcing”). This includes, for example, the following aspects:

- Which risks for business operations result from a **dependence** on the outsource partner? Are these problems considered in business continuity planning and contingency management? Measures taken by the outsource partner in the field of business continuity planning, disaster recovery and data backup also have to be included in the overall consideration of the situation.
- Are the provisions governing essential aspects of the **contractual relations** between credit institution and IT service provider sufficiently clear and detailed? This concerns, in particular, the conclusion of binding service level agreements with precisely defined requirements that are adjusted to the system in question and its importance in ongoing business operations (e.g. with regard to maximum response times and downtimes, maintenance windows, availability of the service provider’s staff for troubleshooting, etc.)? The handling of confidential data also has to be subject to explicit regulations (declaration of confidentiality by the staff of the service provider, etc.).
- Does the outsourcing credit institution have adequate **control rights**? Checks can be performed by employees of the outsourcing enterprise or by external experts. The certification of the service provider according to a quality and/or security standard forms a certain basis for limiting specific risks, but should not be the only measure taken in this field.

The question of **IT audits** has to be studied separately due to the specific expertise required. Smaller audit units frequently will not have the necessary know-how for performing an audit on the IT environment to the extent required. In that case, external auditors (appropriately qualified personnel of audit associations or specialized IT audit enterprises) may be used. Above a certain size, institutions will find it worthwhile to reflect on whether the related competence should be built in their own internal audit unit. At any rate, a regular review of the IT field – with a special focus on security aspects – is a recommendable complement to the overall security concept and, therefore, should form part of any security policy.

### 3.3 Business Processes

#### 3.3.1 Risks – Business Processes

When studying operational risks resulting from business processes, the first step is to distinguish those cases in which the risk is not due to the organization of the process itself (process failure), but to the persons in charge of its performance (human error). Thus, the following cases can be identified:

- Processes with a **faulty overall design** involve a great potential of operational risks. These cases are typically found in areas in which processes are historically grown without a corresponding development of procedural organization. Business fields particularly vulnerable to this type of process risk are those characterized by a high dynamism and/or fast growth because

the rapid development of day-to-day business leaves little time for establishing formal structures. Instead, transitional solutions and improvised mechanisms become the rule in the course of time; due to lacking resources, they are not subject to methodical reviews or revisions. Such a proliferating patchwork in process organization may also arise when new products are introduced and new markets or business lines are opened up. This problem may take on the following forms:

- Processes without clear definitions, for example, when insufficient time was spent on documenting them;
- Outdated process descriptions in cases where “reality” already strongly differs from the guidelines laid down in the past; and
- The extreme case of a completely missing documentation.

In all these cases, there is a risk of rising error frequency, especially when new employees are put in charge of a process as an inadequate or lacking description makes it more difficult for them to get started. In cases differing from previous routine, an inadequate process description hardly offers any indications on how to handle an exceptional situation, which also dramatically increases the risk potential: improvisation could give rise to major mistakes, while a problem completely neglected due to missing guidelines also has adverse effects in most cases (e.g. a customer complaint is received, but then neglected as there are no rules on what to do or how to proceed in such a case).

- In a process, certain circumstances may occur that result in an **elevated operational risk in a certain part of the procedure** – sometimes only a single process step. Such risk factors also exist in sound, well-developed processes since they sometimes cannot be avoided due to the subject of the process or due to technical circumstances. When existing weaknesses and risks are analyzed, however, they have to be given special attention. Some examples are:
  - **Media changes**, i.e. the transfer of information from one medium to another. Frequently due to technical reasons, media changes involve the risk of mistakes being made during transfer, especially from manual to automated processing and vice versa. Wherever possible, such changes should be avoided; if they are unavoidable for technical reasons, appropriate control measures are recommendable.
  - **Transitions from one organizational unit to another** are also typical risk-prone steps within a process. Due to the traditional focus on organizational units (each division has certain competences and responsibilities and concentrates on its own tasks), interfaces between fields of responsibilities are sometimes neglected. Thus, it might occur that, for example, a control step is omitted because both units assume that the other unit was responsible for it. Data might also be supplied in a form necessitating additional work at a later stage in the process, which could be avoided by a minor change in data production. But as these data have “always” been produced and received in that form, adjustments are not made.
  - **Bottlenecks in a process** are frequently caused by insufficient resources (e.g. lacking of specialized knowledge) or inadequate delega-

tion. In addition to the potential negative effects of such bottlenecks on processing speed, they also increase the consequences of a failure regardless of whether this relates to an employee (see chapter 3.4) or a system (see chapters 3.1 and 3.2).

- **Redundancies in processes** occasionally are caused by historical developments, e.g. when a division retains responsibility for performing a control measure or a processing step even though another unit is entrusted with the same or an equivalent responsibility. Such duplication always reduces processing speed.

In the context of significant business process risks, **standardized high-volume processes** have to be distinguished from **individual processes**. Both types occur in the business practice of credit institutions, e.g. the processing of massive quantities of orders on the one hand and the activity of a portfolio manager in asset management on the other hand.

In retail business, heavily standardized processes prevail, which naturally are well suited for IT support. Such technical solutions usually have a positive effect on process quality since automatic control mechanisms can be provided and, moreover, media changes and the like can be avoided. However, especially in the case of processes involving a high number of transactions and additionally marked by a high time pressure, such controls may be bypassed in practice (or perhaps even have to be circumvented in order to cope with the workload). The “four-eyes principle” enforced by appropriate system functions (confirmation of input by another user), for example, might prompt employees to exchange their passwords – in violation of existing guidelines – so that transactions are processed without delay. This renders the control measure ineffective and, what is more, password disclosure in itself constitutes a risk. Furthermore, the introduction of IT systems to support business processes may open up an additional potential of operational risks due to the dependence on electronic data processing (see chapter 3.2).

Areas that are characterized by individual procedures differing from case to case constitute a special challenge to process organization and documentation. Because it is very difficult to develop detailed instructions for such processes, the skills of the employees involved in the processes are of major importance. Therefore, special consideration is to be given to the “human” risk in the operational risk assessment (see chapter 3.4).

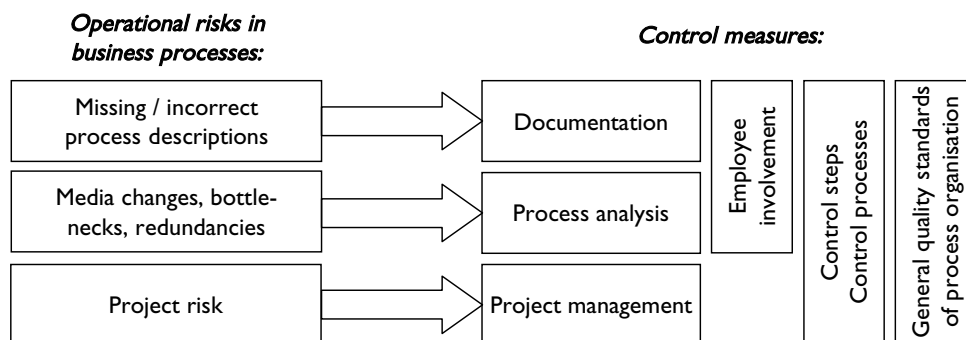


Chart 3.3: Several Typical Operational Risks in Business Processes and the Related Control Measures

A specific type of risk also exists for one-time activities of a limited duration carried out to reach predefined objectives, i.e. **projects**. Here, the hazard mainly results from the uniqueness and, thus usually also from the novelty of such activities. Without appropriate regulations on project work, the following risks may occur:

- An unstructured and unsystematic procedure creates the risk of improvisation with uncertain success. Thereby, resources are blocked for an unspecified period of time; eventually, a project might peter out (end without any results) so that the expenses incurred are lost.
- Unclear or undefined powers to give directives and reporting duties increase the risks in this field: a project's implementation is rendered significantly more difficult if project managers are not in a position to assign tasks in a binding way and/or to monitor progress. Delays or bad planning resulting therefrom may raise project costs or even endanger overall success.
- Shortcomings in planning and coordination may lead to problems when employees have to meet requirements of day-to-day business and cope with the additional workload of project management. This results not only in conflicts between project managers and their superior line manager, but also in risks related to insufficient human resources (elevated risk of error, etc., see chapter 3.5 "General Risks – Staff"). Disputes arising from such resource conflicts paralyze not only project work, but may also impair regular business operations.

### 3.3.2 General Measures – Business Processes

To reduce the risk potentials mentioned above, measures of process organization are required that could be put under the responsibility of a separate organizational division or, for example, of a relevant staff unit (depending on the size of the credit institution).

The sound **documentation of business processes** is a basic requirement for a well-functioning process organization. Care is to be taken to keep the process descriptions up to date and clear; furthermore, it is important that the documentation does not only exist, but also is made accessible to the employees in as simple a way as possible. The risks of undocumented or poorly documented processes have already been described above; appropriate process descriptions, however, also help new employees to become acquainted with their tasks and permit a systematic adjustment and optimization of processes when process organization, business activities or framework conditions change.

With regard to the documentation's form, it is to be borne in mind that its type and volume should be proportionate to the size of the institution and the complexity of its business activities. An excessively detailed documentation may even be counterproductive since a huge amount of information discourages users (from reading the process descriptions so that they become ineffective); moreover, maintenance requires more efforts resulting in the risk that processes are updated belatedly or not at all.

Ultimately, it is of secondary importance whether textual descriptions or graphic representations are used as long as the documentation is up-to-date,



clear and, above all, easily accessible. The question of whether tools, such as process modelling software, knowledge management systems or intranet publishing solutions, should be used has to be decided in line with the circumstances and requirements in each individual case.

Weaknesses and risk factors within the processes can be detected and avoided by means of process analysis techniques described in the relevant literature (ranging from documentation review and analysis workshops to methods like FMEA (see box) and IT-supported analysis and simulation techniques). A systematic examination of the work process in its entirety can eliminate, in particular, the difficulties arising from responsibility boundaries between organizational units. Extensive and comprehensive interface analyses help to resolve problems that frequently occur at organizational and/or technical interfaces. Moreover, this permits a targeted search for risk factors and hence, a significant step towards optimized processes.

#### **FMEA (Failure Mode and Effect Analysis)**

*The Failure Mode and Effect Analysis examines possible failures at a product or service level and assesses their potential effects on customers. Failure-effect chains are analyzed at various process levels. This preventive method is to help avoid failures critical to customers by the early identification of failure sources. One of its characteristics is that it links products and processes.*

*FMEA can already be applied in process design. As a continuous process FMEA, it may focus on weaknesses in business processes and, in the form of a system FMEA, it may examine the interaction of subsystems and identify potential weaknesses, for example, at interfaces.*

*Risk priority numbers that are obtained by multiplying the scores for:*

- *the probability of occurrence,*
- *the severity, and*
- *the probability of detection*

*serve to define the priorities for taking measures.*

*Within the framework of operational risk management, this method is mainly suitable for risks that occur more frequently and have low to medium effects.*

At any rate, it makes sense to define **clear responsibilities for the further development of processes**. Various solutions are possible – from centralization in a separate organizational unit to a decentralized approach in which the process owners in the specialized divisions are given the required competence and take on responsibility for ensuring that the processes work well and are improved. Mixed forms are possible as well.

To **involve the employees** in the system of process organization, appropriate training measures have to be arranged – for new employees as well as for all employees upon major changes; please note again the great importance of an accessible and simple process documentation. The continuous improvement of business processes can also be supported by suitable measures (e.g. in-house suggestion schemes) in order to benefit from the know-how and experiences of those using the processes every day.

Within the processes, **control steps** are to be planned at suitable points, which – being preventive measures – are to help detect and correct failures already during process runs. It is to be borne in mind that the frequency and intensity of these control measures must be adjusted to the requirements of



the relevant process in order to limit the risk as much as possible as well as to avoid that the process becomes cumbersome due to excessive controls. In many cases, the need for certain control steps (e.g. “four-eyes principle”) will already result from legislation, minimum supervisory requirements or international standards; such measures have to be implemented at any rate. The most appropriate type of control step has to be assessed according to the specific case in question; possible options are:

- Parallel control, in which processing steps are performed at the same time and the results are compared;
- Serial control, in which results obtained at different points in time are compared;
- Redundant control, which requires that a processing action is repeated for control purposes in order to make sure that the result is correct; the control may be performed in parallel to processing or later on (serial control); and
- Plausibility checks examining the consistency of the result in line with pre-defined rules.

In addition to these control steps within the processes, separate **control processes** – a second level of quality assurance, so to speak – usually also have to be provided depending on the requirements of the business line in question; this category, for example, includes coordination processes in the field of settlement, balance comparisons, etc. Attention has to be paid to segregating responsibility for process implementation and control (see also chapter 3.4.3). For all controls and, in particular, this type of controls, it is to be borne in mind that under the Labor Charter<sup>65</sup>, certain measures require the involvement or even consent of the works council.<sup>66</sup>

In this context, the **internal audit function** plays a special role since the examination and control of business procedures is one of its core tasks. Its control activities not only relate to value-creation processes but also to processes forming part of the internal control system. As a result, the internal audit function is an important second control layer in the overall system of process control. The activities of the **compliance function** are also worth mentioning because it is in charge of an important control process relating to securities transactions for the enterprise’s own account, customer transactions as well as staff transactions. The management of conflicts of interest also has to be seen as having a function related to business process control.

Because, even in ideal cases, failures can never be fully avoided provision has to be made for **cases deviating from the norm defined**. Thus, processes must not be developed exclusively for flawless normal cases (“fair-weather processes”), but rather have to include procedures regulating the handling of mistakes: correction measures, escalation processes, etc. This is the only way to ensure that reasonable measures are taken to limit losses when

<sup>65</sup> Bundesgesetz vom 14. Dezember 1973 betreffend die Arbeitsverfassung, Federal Law Gazette No. 22/1974, as amended.

<sup>66</sup> For example, information duty regarding automation-supported recording of employee data (Article 91 paragraph 2 of the Labor Charter) or the duty to obtain consent to control measures and technical systems for controlling employees if these measures (systems) affect human dignity (Article 96 paragraph 1 item 3 of the Labor Charter).

problems arise; moreover, the systematic analysis of such failures makes it easier to avoid similar incidents in the future.

Both control steps and control processes are tools of **historical control**, while process analyses mentioned above are a type of **forward-looking control**. The objective of establishing **general quality standards in process organization** is pursued by linking both types of controls in a comprehensive quality assurance system. Such systems, some of which are based on international standards (e.g. ISO 9001:2000) while others were developed in practice (e.g. Six Sigma and Total Quality Management), provide a comprehensive package of measures to achieve a high quality level. One of the benefits of such programs is that they have been applied in practice and further developed over a long period of time so that individual enterprises need not reinvent the wheel, but can rely on well-proven, comprehensive methods.

#### **ISO 9001:2000**

*The ISO 9000 standard series issued by the International Organization for Standardization is comprised of standards on quality management and quality assurance for processes in enterprises. The process-oriented standard frequently used as a basis for certification is ISO 9001:2000, the current version adopted after the most recent revision in the year 2000. Its objective is the continuous improvement of the quality management system and, hence, the products and services to raise customer satisfaction, a stronger orientation to business processes and the application of several management principles in designing the quality management system.*

*Some requirements defined for business processes in this standard are of interest for all banks. According to the standard, an organization should, for example:*

- identify the processes required for the quality management system and their application within the organization,*
- determine the sequence and interaction of those processes,*
- define the criteria and methods needed to ensure the effective performance and control of those processes,*
- ensure the availability of resources and information required for supporting the performance and monitoring of those processes,*
- monitor, measure and analyze those processes, and*
- implement the required actions to achieve the results planned and a continuous improvement of those processes.*

#### **Six Sigma**

*Six Sigma is a process and quality management method aiming at making processes almost error-free. It analyses and breaks down processes in such a way that they can be submitted to a statistical analysis. Six Sigma helps to identify “Critical to Quality” (CTQ) characteristics in processes. In statistical terms, Six Sigma means that in fact, only a maximum of 3.4 defects results from one million opportunities and ultimately aims at achieving processes of zero-defect quality.*

*Six Sigma may be used for existing as well as new processes. For this purpose, basically two methods were developed that constitute a cyclical, iterative sequence of processes and are implemented in the form of projects:*

*DMAIC*

*define, measure, analyze, improve, control; and*

*DMADV*

*define, measure, analyze, design, verify.*

*The method was originally developed in manufacturing companies. Meanwhile, Six Sigma is also used in service-sector enterprises, such as banks and insurance companies, to optimize standardized processes with high transaction volumes that have characteristics similar to industrial production processes. By avoiding defect cost, high expenses on eliminating defects can be saved. These may reach a considerable level in the back-office area of a bank, if you think, for example, of the cost of manual corrections of wrong account entries or incorrect money transfers.*

The introduction of such a system or standard regularly involves great efforts so that one has to critically examine whether those efforts are justified by the expected benefits. In most cases, this will hold true only for credit institutions of a certain size. Another aspect to be considered is that a comprehensive quality assurance program always needs the management's support in implementation and must be integrated into corporate culture. Introducing such a system as an end in itself, for example to obtain a quality certificate, frequently does not result in the desired effects in reducing failures in process organization. Instead, excessive documentation, too complicated structures or inadequate involvement of employees in the change process may create new risk potentials.

### 3.3.3 Special Measures – Business Processes

**Risks related to project work** can and should be addressed using means of process organization as soon as projects exceed certain proportions within a credit institution. Although the unique character of each project makes it difficult to develop a generally applicable, standardized process, it is still possible to define processes for project organization and implementation and to make them mandatory in order to address the specific risks related to projects. Examples are project planning and controlling processes as well as defined notification and reporting paths. During planning, care has to be taken not to compromise the requirements of day-to-day business; escalation and decision-making mechanisms have to be provided for cases of bottlenecks or other resource conflicts. The higher the frequency of project work in an organization and the more complex the projects are, the more detailed regulations should be defined for the procedure to be followed in projects.

This aspect is particularly important for IT projects, which strongly benefit from a methodical approach and tight project management due to their complexity and numerous interfaces between engineers and specialist divisions. Additionally, such projects also have to take account of problems related to IT quality assurance (see chapter 3.2).

**Individual processes**, which require a high level of expert knowledge in most cases and are difficult to bring into a procedural scheme, constitute a special challenge when attempting to tackle process risk. As the concrete procedure varies depending on the circumstances of each individual case, traditional techniques of process analysis and optimization do not yield useful results. It will make sense to include certain quality assurance mechanisms in such processes; the most appropriate measures for this field, however, will rather address the employees involved (ensuring that the required skills are available, etc.) so that reference is made to chapter 3.4 in this context.

Finally, **legal risk** also has to be considered in connection with processes. Especially in cases that touch, for example, issues of consumer protection or supervisory regulations, it is recommendable to involve the legal division, above all when new processes and products are developed (see also chapter 3.7.3 “Measures in the Field of Legal Risk”).

## 3.4 Staff

### 3.4.1 General Risks – Staff

The risks discussed in this chapter include all areas in which the human factor is the key source of risk. Actions of persons not employed by the credit institution, however, are considered to be external influences so that they constitute external events (see chapter 3.5). Only those cases in which a mistake or deliberate action of an employee made the criminal act of the external person possible or at least significantly facilitated it are taken into account in the present chapter.

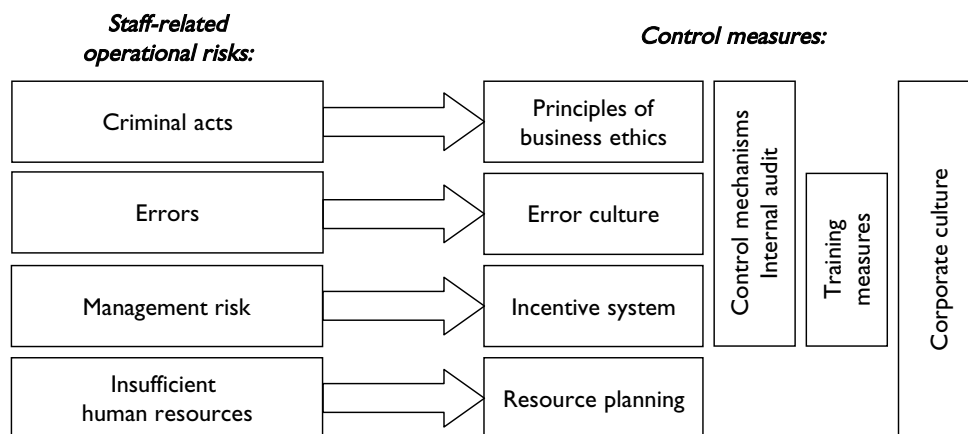


Chart 3.4: Some Aspects of Staff-Related Operational Risk

The main risks falling under the category of staff risks are:

- Risks due to criminal acts of employees, i.e. typically acts committed with the intent to make personal gain and/or to cause damage. Such staff offences are by no means seldom exceptions, but are relatively frequent in practice, with the number of unknown cases probably being rather high as well.<sup>67</sup> In many cases, external offenders will also be involved. The most important offences are:<sup>68</sup>
  - Larceny, misappropriation or embezzlement of funds or fixed assets;
  - Fraud;
  - Corruption, i.e. the acceptance of advantages offered in order to make employees act in a specific way (contrary to their duties); and
  - Computer crime, such as data theft, manipulation of IT systems and data corruption.

<sup>67</sup> Franke, Der Feind in den eigenen Reihen, 2004.

<sup>68</sup> Ernst & Young, Studie: Wirtschaftskriminalität in Deutschland, 2003.

- Criminal acts may be directed against the employer – i.e. the credit institution – or third parties (usually a customer). In the former case, the bank is directly harmed, while in the latter case, a concrete loss event in terms of operational risk only exists if the credit institution is liable for the employee's act.
- All human activities harbour the risk of error; the more complex an activity, the higher the risk. As a result, the risk of damage due to **mistakes** is extremely varied; the spectrum includes cases such as incorrect processing due to insufficient expertise, clerical mistakes, wrong inputs in IT systems, omissions or errors due to work-related or private stress, etc. In contrast to criminal acts, these mistakes do not involve any intent to make personal gain or cause damage to the employer or third parties. If the credit institution itself is the party harmed, the special regulations of the Employee Liability Act<sup>69</sup> have to be applied, which strongly limit the employer's claims against employees on the grounds of negligence ("inadvertence"). If an employee causes damage to a customer of the credit institution, the provisions on vicarious liability (Article 1313a of the General Civil Code – *Allgemeines Bürgerliches Gesetzbuch*) will apply as a rule so that the bank has to indemnify the customer, while its recourse against the employee again is subject to the restrictions of the Employee Liability Act.
- A special risk also arises from **insufficient human resources** since the resulting higher work load of the existing employees increases the risk of errors (due to insufficient expertise or time). Moreover, the pressure exerted on the employees due to tight personnel resources leads to stress and, subsequently, often to frustration – two factors raising the risk level. Such a lack of staff in a department or division may, for example, be a consequence of extraordinary high business growth or cost reduction measures.
- If staff requirement planning does not take account of the possibility of **sickness leave** or **termination of employment**, short-term human resource problems may arise.<sup>70</sup> Such sudden bottlenecks increase the pressure on the remaining employees; furthermore, there is the risk that transactions already underway are not further processed and special know-how and skills are no longer available – if employment is terminated, the specialized knowledge of the employee in question is even lost permanently. At certain times of the year ("influenza season"), a high number of employees must be expected to be on sickness leave, which may have a rather strong influence on day-to-day business.
- Finally, **management risk** has to be mentioned, which relates to potential losses caused by criminal acts or mistakes made at the management level. This risk does not constitute a separate risk category and has the same variants as the ones presented above for staff risk in general. Given the powers of executives and the possible severe consequences of mistakes made at that level, however, the damage potential may be considerable so

<sup>69</sup> Bundesgesetz vom 31. März 1965 über die Beschränkung der Schadenersatzpflicht der Dienstnehmer, Federal Law Gazette No. 80/1965, as amended.

<sup>70</sup> See Kraft/Balduin, Risikofaktor Mitarbeiter, 2002.

that it seems to be appropriate to take special account of this risk. Some failures occurring at the management level, nevertheless, rather fall under strategic risk (see chapter 1.2 “Definition of Operational Risk”), e.g. activities in a new business line whose special risks are not fully recognized and, therefore, not adequately limited. Those cases must not be neglected due to their significant loss potential, but they are not covered by the definition of operational risk according to Basel II. Thus, when examining risks in this field, efforts have to be made to ensure as accurate as possible a differentiation between strategic risk and operational risk.

### 3.4.2 Special Risks – Staff

Naturally, staff risk has to be given special attention in those business lines in which major assets are at risk because this could not only make criminal acts more tempting, but also aggravates the impact of failures. Examples of **high-risk business lines** are foreign exchange and securities trading, which is also confirmed by well-known cases of highly striking loss events caused by operational risk in the recent past. Depending on their importance for the business activities of a credit institution, support processes (e.g. in settlements) may also have a high risk potential.

Furthermore, numerous cases have shown that individual employees may become particular risk factors due to their special position and skills. These “**risky stars**”<sup>71</sup> are characterized by the fact that they acquire a kind of “hero” status because of their extraordinary success, which allows them to ignore existing rules and control mechanisms. The above-average results they achieve, so to speak, block the view; their superiors and control units actually do not want to challenge the star’s actions in detail as long as the results are excellent. Of course, the greater leeway given to these persons creates an immense risk potential. A typical example of such a high-risk person is a trader who regularly exceeds limits with the consent of his superiors due to extraordinary trading profits or even starts to trade in products whose risks are not or insufficiently limited in order to raise the chances for further above-average profits.

Another type of “high-risk employee” is a **key player** who has exclusive knowledge and skills in a certain domain (of particular importance in most cases). Because of the resulting bottleneck, the risk that this person is not available – at worst due to termination of employment, but perhaps already due to a prolonged vacation – is of considerable importance. Examples are employees in the IT field who have exclusive knowledge about insufficiently documented key systems.

### 3.4.3 General Measures – Staff

One of the most important measures related to all types of staff risk certainly is the establishment of a **corporate culture** reducing such threats. This requires a constructive way of dealing with mistakes. After all, when the first response to a failure is an immediate search for culprits, there is a risk that such incidents are not talked about or even hushed up. As a result, it is more

<sup>71</sup> n.n., Risky Stars, 2002.



difficult to collect loss data and, what is more, it is impossible to learn from mistakes, search for their causes and take targeted preventive measures. Moreover, socio-psychological experiments show that persons who feel that they are treated unjustly are more likely to take “revenge” so that, for example, the frequency of fraud increases.<sup>72</sup> Thus, the climate and culture of a credit institution also influences staff risk in this respect.

On the other hand, an appropriate corporate culture can also reduce the risk of deliberate failures if **principles of business ethics** are not merely proclaimed, but practiced in the credit institution. Although this approach is by no means a cure-all, it still is a possibility – yet difficult to attain – to mitigate certain risks. Demands for voluntary compliance with a code of conduct go in the same direction: a climate is to be created that is characterized by honesty and trust.<sup>73</sup>

All measures related to corporate culture, however, require significant implementation efforts. A rethinking process, which is usually necessary to achieve such changes, is time-consuming and also very difficult to initiate from the top down. As an interface between the management and the staff, the works council can have a significant role to play here.

Another essential component are control mechanisms that aim at the early detection of failures and at making deliberate manipulation as difficult as possible. Under the motto that it is good to trust, but better to control, such measures include:

- Establishment of **approval and control steps** in business processes as well as creating separate **control processes** (see also chapter 3.3 “Business Processes”);
- Mandatory **documentation** of certain actions and transactions so that the precise circumstances can be tracked later on; such mechanisms may also be supported by technology (automatic logging of database accesses, transactions, etc.); and
- Measures related to the organisational structure, in particular the **segregation of functions** to prevent that a person supervises his/her own activities (elevated possibility of error or manipulation) or is exposed to conflicting objectives specific to different functions he/she fulfils.

For minimizing the potential abuse of sensitive information as well as reducing the risk of inadvertent damage in this field (unintentional deletion of data or disclosure of confidential information), a key step is to ensure as much as possible compliance with the **need-to-know principle** according to which employees should only get access to data they need for fulfilling their professional tasks. Thus, access to sensitive information is blocked on principle and only explicitly permitted in those cases in which it is necessary. Proceeding the other way round (information not explicitly blocked is accessible) harbors the risk that access restrictions are forgotten.

A common and useful instrument to reduce errors are diverse **training measures**. These include education and training activities providing the

<sup>72</sup> V. Heyden, Mitarbeiterkriminalität – Umfeld und Hintergründe, in: Die Bank, April 2004.

<sup>73</sup> See also Romeike, Risikomanagement jenseits der exakten statistisch-mathematischen Methoden, 2002.



employees with the required qualifications for their activities, courses of a special risk-mitigating nature (e.g. first-aid courses, seminars on the prevention of money laundering or fraud) as well as information events to raise the staff's risk awareness and reinforce other measures of risk mitigation (see, for example, the explanations on measures to raise awareness of IT security in chapter 3.2).

Risks related to insufficient human resources eventually have to be addressed by appropriate **resource planning** taking account not only of the general requirements of business activities, but also of special factors, such as seasonal fluctuations of business volume and the number of persons on vacation or sickness leave or particularly high growth in certain business lines. In the context of personnel management, the training measures mentioned above also have to be planned in order to ensure that all employees get the training they need.

Finally, **internal audit** plays a special role in identifying and mitigating staff-related risks. In this context, internal audit is supported by the **compliance function** that is responsible for supervising securities transactions carried out by employees for their own holdings. One objective of these activities is to protect the enterprise against unexpected risks from improper or non-compliant actions performed by employees with regard to their own securities holdings.

#### 3.4.4 Special Measures – Staff

In areas with particular risks due to high loss potentials, **special controls and precautions** have to be provided. Examples of such measures are the application of the “four-eyes principle” for certain work steps, a mandatory confirmation of trading transactions by an independent unit and not by the trader as well as a non-modifiable log of transactions in production systems.

Processes requiring specialized **expert knowledge** necessitate that particular attention is given to the availability of the related know-how and skills. Since the uniqueness of such processes makes it difficult to control quality by individual routine checks, all the more care has to be taken to ensure that the people working in these areas not only have the required knowledge, but also can maintain and update it. This is of particularly high importance for topics subject to rapid change, e.g. taxation law, information technology, derivatives transactions (see the explanations on individual processes in chapter 3.3 “Business Processes”).

To **prevent bottlenecks related to specialized knowledge and skills**, it is also necessary to identify key personnel and adopt rules of replacement ensuring that business activities are not seriously impaired by the short-term unavailability of such a person. At any rate, a concentration of specialized knowledge in a single person has to be avoided, especially if insufficient documentation or the complexity of the subject field make it difficult to rapidly break in a substitute. While it is still relatively easy in small and medium-sized organizations to keep an overview of who has specialized knowledge, this is more difficult in big organizational structures. In those cases, knowledge management techniques (e.g. knowledge maps) and other methods can contribute to identifying bottlenecks and initiating appropriate measures.

**Approaches of incentive and motivation theory** may also be applied to control and limit staff risk. On principle, such considerations, which are based on psychological findings on human behaviour in groups (role behaviour, communication theory, etc.) or typical reactions to a reward or sanction system, are nothing new; however, their application as instruments of operational risk management is still in its infancy. At any rate, such approaches contribute to a comprehensive consideration of the human factor that is extremely important for operational risk.

### 3.5 External Events

#### 3.5.1 General Risks – External Events

The information presented in the following chapter may overlap with the contents of the previous chapters since it is obvious that many external risks can be addressed and mitigated by organizational, infrastructural, process- or staff-related measures taken in the framework of operational risk management. This applies to damage caused by the elements (e.g. fire) covered by precautions taken within the enterprise that at least have a damage-reducing effect also for external threats (neighbouring buildings, vandalism), as well as to all cases of external crime (fraud, larceny, robbery, etc.) for which there is a certain residual risk even when all relevant measures and mechanisms have been taken. Therefore, security issues related to persons, values and buildings have been discussed under the headings of infrastructure, business processes and staff behaviour. Exotic examples of these risks also include war-related and political risks as well as, unfortunately rather topical, risks from terrorist acts against which measures are only possible to a limited extent and, at any rate, have to be highly specific to the enterprise in question.

The risks falling under the external category cannot be listed exhaustively, but should by no means be neglected. Each credit institution has to identify the relevant operational risks with external causes and analyze them also with a view to potential serial risks.

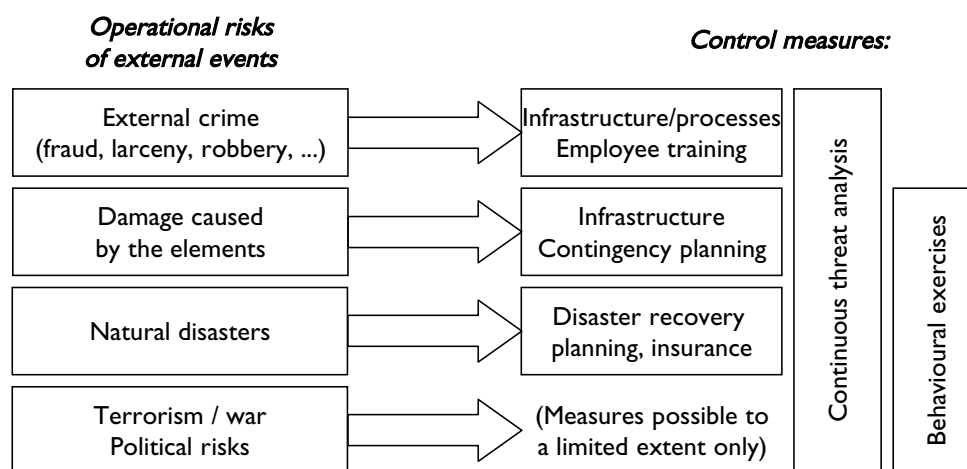


Chart 3.5: Key Operational Risks Caused by External Factors

Purely external events, i.e. those that are not partly due to internal causes nor primarily manageable by general measures described in the previous chapters, include **natural hazards**, i.e. environmental and weather influences in the broadest sense as well as their consequences, especially if they exceed certain proportions (**natural disasters**). A natural disaster in a narrower sense is a serious event caused by the elements in the planetary<sup>74</sup>, atmospheric or terrestrial environment affecting the enterprise's functioning that is capable of resulting in substantial or more or less large-scale losses of human life and/or property and which, due to the magnitude of damage, is unlikely to be fully managed by the enterprise itself. Nevertheless, it is possible and necessary to plan forward-looking measures also in this field since it is not only the economic existence of the enterprise, but also primarily the safety of employees and customers that is at risk.

Risks related to **external crime** also belong to the category of external events although they may also be connected with internal hazards (staff risk). Criminal desires triggered by the values held by banks have always formed part of the threats faced in banking. This is true for robbery, larceny and burglary as well as for all types of fraud. With regard to fraud, however, a differentiation has to be made since in addition to diverse variants of bank fraud, i.e. fraudulent actions with the aim of causing damage to a bank, fraud against bank customers may also constitute a risk for the credit institution. The relevant cases may range from defrauders merely using bank accounts to the clever and targeted exploitation of technological or product innovations – and frequently of the sound reputation of a bank – by criminals to cause damage to their victims. In this respect, special mention needs to be made of IT risks, such as security issues in online banking.

Furthermore, banks at least **share responsibility** for certain criminal threats to which their customers are exposed and that need not be limited to their premises. In this context, reference is to be made to a tendency in court rulings<sup>75</sup> according to which banks have to maintain privacy to protect their customers under their ancillary contractual duties. In particular, when higher amounts of money are paid out, protection and warning duties will have to be borne in mind.

In the area bordering on staff and process risks, there are finally **external risks for employees** that exist on principle at work or off work and may lead to a temporary or permanent loss of staff (epidemics, natural disasters, terrorism, force majeure, etc.). These risks have to be addressed under the heading of staff risk and limited by designing processes appropriately (rules of replacement, representation powers).

### 3.5.2 Special Risks – External Events

In Austria, natural hazards include: earthquakes, movement of masses (earth flows, mud slides, avalanches), soil subsidence, storms (winter gales, torna-

<sup>74</sup> An example of an interplanetary event are the effects of a meteorite impact: in their direct form, the effects go far beyond the scope of all measures that can be taken at the enterprise level, but secondary effects, such as the failure of satellite communication due to these phenomena (e.g. blackout caused by the Leonides meteor shower) have to be taken into account.

<sup>75</sup> For example, decision of the Austrian Supreme Court in the case 6 Ob 77/05z of June 23, 2005.

does, blizzards), lightning, heavy precipitation (heavy rain, snowfall, hail), floods (river floods, flash floods), frost and forest fires.

The real threat must not be underrated: the country profile established by the Munich Re Group for Austria, for example, shows a medium to above average risk of earthquakes, winter storms and lightning for the entire country, a largely high risk of hail and, with regard to floods, strong variations of risk – due to the dependence on local factors –, but at least a medium risk for one third of Austria.<sup>76</sup>

- **Earthquakes** are commonly considered to be the most destructive natural force – perhaps because their victims suffer the strongest shock (in terms of economic damage and the number of deaths, however, they are by far exceeded by storms and floods all over the world). The most severe direct effects of earthquakes are the destabilization or destruction of buildings, but indirect effects such as earthflows, damage to pipes (gas, water), shorts and/or fire have a comparable damage potential.
- In Austria, thought is to be given to **storm damage** caused by so-called winter storms (possibly snowstorms) and katabatic winds (foehn) as well as electric storms (thunderstorms, hailstorms, blizzards). In the Alps, storms may also be a reason for avalanches building up and being triggered.
- The most frequent direct effects of **lightning** and **thunderstorms** are fires and damage to electric equipment due to voltage surges or melting. Considerable secondary damage has to be expected, e.g. failure of power supply, IT or telephone networks, perhaps even at a larger scale if entire power plants or parts of the electricity network fail.
- **Precipitation** (rain, hail, snow) can cause a variety of damage: While strong rainfall may lead to water entry, flooding, earthflows or mud slides, hail causes destruction directly during precipitation. Snow may destabilize buildings due to its weight, build up an excessive load on power supply and communications lines or obstruct roads for a longer period of time.
- In Austria, **flooding** is caused by river floods and strong rainfalls and often results in enormous damage on a macroeconomic scale. It occurs more or less along rivers after strong precipitation in larger regions or, in the Alps, due to flash floods after heavy rainfall or thunderstorms or due to snow melting. Effects such as a rise in the water level of lakes and groundwater reservoirs may also have adverse consequences. Flooding causes immediate and irreversible damage to goods vulnerable to water (e.g. computers, but also assets held in custody), while damage to buildings, as a rule, depends on the type and duration of flooding.

The concrete threats faced by a bank due to **external crime** has many faces: in addition to the bank-specific forms of larceny and robbery, consideration has to be given above all to different variants of bank and customer fraud due to the increase in non-cash payments, but also to special types of crime such as organized crime, including in particular money laundering. In part, legal risks additionally arise from relevant provisions of the Banking Act and other liability regulations. Moreover, all types of external crime to which banks may be exposed tend to have a higher damage potential as soon as a bank employee is

<sup>76</sup> Münchener Rückversicherungs-Gesellschaft, Welt der Naturgefahren (2000).

the offender (internal fraud) or an accessory (often due to a staff risk, e.g. vulnerability to blackmail, gambling addiction, debts).

- First of all, **larceny, burglary and robbery** – the classic crimes against property – have to be mentioned. Robbery may reach a particularly severe level when hostages are taken or special brutality is used. This category also includes all known types of bank holdups, but also relatively new developments, such as blasting or “towing” away of automated teller machines (ATMs).
- **Fraud**, in its diverse forms, constitutes a very wide spectrum of threats for banks: it may be committed by kiting or forging checks, bills of exchange, securities or letters of credit, in connection with account opening, transfers or direct debiting transactions, in the form of credit fraud (also in combination with forgery of annual financial statements or fraudulent insolvency) or assignment fraud. Due to the key role played by credit institutions in cash circulation, counterfeit currency also constitutes a significant risk.
- The widespread use of IT systems in banking increases the importance of **cyber crime** in all its forms. This relates first and foremost to unauthorized external access to the systems of credit institutions in the intent to manipulate software or data and to spy out data. This category also includes data corruption as a form of IT sabotage, which may cause major damage.
- The specific features of the internet and e-banking, however, also make it possible for criminals to target **bank customers** with their activities. An example is “phishing”, i.e. the attempt to fraudulently acquire passwords from customers, for example, by seemingly official e-mails of the credit institution. In some cases, even perfect imitations of bank websites are produced in order to make bank customers input their personal and account data or passwords on fake online banking pages (“pharming”) to be used, for example, to steal money from their accounts or damage them in similar ways. Techniques, such as “DNS spoofing”, can even redirect a correct access to the bank’s website to a fake version. The direct victims of such activities are the customers of a credit institution, but it is very well possible that the bank – if it does not meet its duty of due diligence – has to compensate customers for damage incurred. Of course, such incidents also highly endanger a bank’s reputation. This is similarly true for other fraudulent ways of obtaining access authorizations, e.g. manipulation of ATMs or other self-service facilities.
- Types of fraud not directly targeting banks, but their customers also include **credit brokerage and investment fraud**. Because, as a rule, both the offender and the victim use bank accounts in the course of the fraud, however, the bank might also violate information duties in this case, which may result in claims for damages (legal risk).
- Another form of external crime which may concern banks mainly in the context of organized crime is **money laundering**, i.e. the performance of diverse transactions to conceal the illegal source of revenue generated by criminal activities. A recent development in this field is the **financing of terrorist activities**. In this context, special reference needs to be made to the relevant provisions of Articles 40 et seq. of the Austrian Banking

Act on the duty of care in combating money laundering and terrorism financing (legal risk).

### 3.5.3 General Measures – External Events

For external events, too, a detailed continuous **analysis of risks and threats** naturally is the starting point and prerequisite of any further preventive measures. A risk analysis appropriate to the size and complexity of a credit institution should consider the key external framework conditions of its business activities, such as geographic location as well as existing infrastructure and processes (in outsourced areas, too) and take into account indicators, such as the crime situation in its business environment.

- The **geographic location** determines exposure to various natural hazards (near rivers, in mountain areas, etc.), but may also have an indirect impact, e.g. at certain sites the percentage of one-time customers is higher (for example, money exchange near train stations).
- In this context, important infrastructural and process-related aspects are the **access options** offered by banks to their customers (personal contact, telephone banking, self-service facilities, online banking), the portfolio of products and services that, as a rule, involve different levels of risk, and the customer structure (new and one-time customers, the bank's own employees, income, sectors, sanction and embargo lists, etc.). For risks resulting from external crime, it is to be borne in mind that infrastructural measures and processes must keep pace with new technologies and the development of business activities in order to remain effective.
- The **crime situation in the business environment** can provide insights into the frequency of certain types of crime and, thus, into the risk situation of the bank with regard to specific threats. In times of internationalization and internet banking, such analyses have to be specified for all sites and access options.

As far as risks related to the natural disasters described above are concerned, the mere disastrous scale of a scenario should not prompt a bank to refrain from protective measures and rely on insurance contracts that in the end might not even provide coverage.<sup>77</sup> Rather, the bank has to deliberately define a scenario with those effects that still can be coped with before all the measures humanly possible and reasonable in economic terms become futile. Disaster management, therefore, refers to the sum of all precautionary and follow-up measures aimed at preventing or coping with a disaster.

For **crises and disaster plans** (evacuating people, fire fighting, securing buildings, business continuity, etc.) to work when needed, they must be documented and communicated and be in line with the organization of the enterprise. As far as the safety of employees and customers as well as business continuity is concerned, exercises to practice the relevant plans are of utmost

<sup>77</sup> Here, the problem of moral hazard frequently arises, i.e. the consequences of a lost incentive to control and prevent risks induced by insurances taken out. However, risk costs are not equivalent to insurance costs. Therefore, active risk management by means of protective measures, disaster plans, etc., is indispensable also in this field



importance in addition to business contingency planning. The following aspects have to be given particular consideration:

- How are responsibilities assigned throughout the enterprise? If responsibilities are dispersed, a coordinating body – or even a reorganization – may be necessary to avoid responsibility gaps.
- Are the human resources and knowledge required available (e.g. safety expert)?
- Are there clear procedures for maintaining and renewing infrastructure?

#### 3.5.4 Special Measures – External Events

With regard to special measures to limit risks from external events and make provisions for them, the highly different circumstances require that each credit institution takes its own special measures whose extent and level of detail depends on the results of the specific analysis of risks and threats. For foreign sites, in particular, all locally relevant hazards have to be taken into account, including risks that may not be important in Austria since they only arise from certain business activities or local threats, such as tropical storms, flash floods, etc. This requires the preparation of special protection measures and codes of conduct for each site.

With regard to the general measures to prevent crime and, in particular, fraud as well as to protect property and people, the following aspects have to be added or emphasized, respectively:

- The significance of **raising awareness**, providing up-to-date **information** (e.g. from bank warnings) and ongoing training of all employees involved in the processes concerned;
- The need for **cooperation** and **coordination** among the units responsible for fraud and compliance (internal/external audit, IT security, money laundering officer, operational risk manager, legal division);
- Transfer of the **KYC (know your customer) principle** from money laundering to fraud prevention; if necessary, this may even include the involvement of the bank's units responsible for combating fraud in the approval of major credits, implementation of large-volume transactions or the outsourcing of services to new or unknown partners;
- Compliance with the “**four-eyes principle**” especially in processes that are particularly prone to internal crime or in which the bank may be liable for negligence (e.g. complete and consistent filling in of letters of credit or checks);
- The use of suitable **IT solutions** where appropriate, e.g. screening accounts for “smurfing” transactions or to compare them with a list of persons identified as defrauders. In the context of IT changes or projects, however, it is to be borne in mind that the transition phase itself results in higher risks; and
- The use of trustworthy internal or external **security services** to protect the premises (especially during high-risk phases such as reconstruction works) and prevent hold-ups and other criminal acts inside the bank as well as during transports. Appropriate measures also have to be taken to protect the customers, especially after they have withdrawn higher cash amounts.



The following special remarks apply to precautions taken with a view to natural hazards:

- **Earthquakes:** A building's earthquake safety depends on its height, year of construction, structure, use, the existence of asymmetric features in its ground and vertical plan as well as, ultimately, on the intensity and duration of an earthquake. As a rule, evacuation will not be reasonably feasible any more. Even after weak earthquakes, the building's structure and piping (gas, water) should be monitored more closely.
- **Storms:** Their effects may require immediate structural measures (parts falling down, new roof). In most cases, damage caused by storms is covered by building insurance contracts.
- **Lightning/thunderstorms:** If compliant lightning protection is installed, there are hardly any measures that can be taken beyond the ones described in chapter 3.1.4 "Special Measures – Infrastructure"; there will always be a residual risk. It is worth noting that, as a rule, indirect effects of lightning – a fire – are covered by a building insurance, while its direct action, i.e. electromagnetic malfunctions (or even destruction) of electronic equipment, is not. For such damage, a special insurance has to be taken out; business interruption insurances may perhaps cover such cases.
- **Flooding:** Special measures naturally depend much on local conditions and range from measures to secure buildings and assets to plans for continuing business operations, for example, in a different building if the flood lasts for a longer period of time. Due to adverse selection, insurances against flood damage constitute a basic problem: those who are located at an exposed site, try to obtain insurance coverage, but do not get it precisely for that very reason (or only at an unaffordable premium).<sup>78</sup> Therefore, most standard building insurances do not cover flood damage.

### 3.6 Legal Risk

#### 3.6.1 General Considerations on Legal Risk

Before discussing aspects of legal risk in greater detail, it is necessary to reflect on its **definition and delimitation**. This is not an easy task since there is no harmonized, generally accepted definition of this risk category; the Basel II regulations, too, only mention legal risk, but do not define it. The explanatory footnote added to the definition of operational risk<sup>79</sup> ("Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.") lists certain aspects by way of giving examples without defining the term as a whole. Likewise, the

<sup>78</sup> In its broadest sense, adverse selection means that "bad" customers (with high risks or weak damage control) naturally tend to be more interested in insurance cover than "good" customers. Because insurance companies cannot simply distinguish between these customer types, the average premium will increase as a rule. However, customers frequently do not take out an insurance against floods if their risk is below a certain threshold (that may well be rather high) so that it is almost impossible to diversify the risk of flooding, which results in a high rise in premiums or no coverage being granted at all.

<sup>79</sup> Basel Committee on Banking Supervision, International Convergence of Capital Measurement and Capital Standards, 2004, p. 644.

EU Directive [2006/48/EC] does not define legal risk, but only states that it forms part of operational risk.

In practice, definitions of legal risk are used that in some cases, are characterized by relatively strong differences and in others, only cover part of the aspects. For example, risks resulting from the unenforceability of contractual provisions (due to insolvency or legal action) or uncertainty in the interpretation of contracts, laws or supervisory requirements are mentioned as legal risks.<sup>80</sup> The following definition used by the Basel Committee on Banking Supervision in some publications constitutes a good, very general approach:

*Legal risk is the possibility that lawsuits, adverse judgements or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of a bank.*<sup>81</sup>

This wording does not list any business lines nor does it specify the type of adverse effects on the “operations or condition of a bank”. This is very well compatible with the fact that legal risk was characterized as a horizontal issue in chapter 1 that does not belong to the major causes (systems, processes, people and external events), but rather pervades them, as it were (see chapter 1.2 “Definition of Operational Risk”): it does not matter whether an “adverse judgement” requires the bank to pay damages due to non-performance of contractual duties or a fine due to non-compliance with regulatory requirements of bank legislation. In this context, it does not make a difference that, under the Austrian administrative penal law, it is not a court, but an administrative authority that decides on fines: such adverse decisions also fall under legal risks just as the “judgements” mentioned in the international definition.

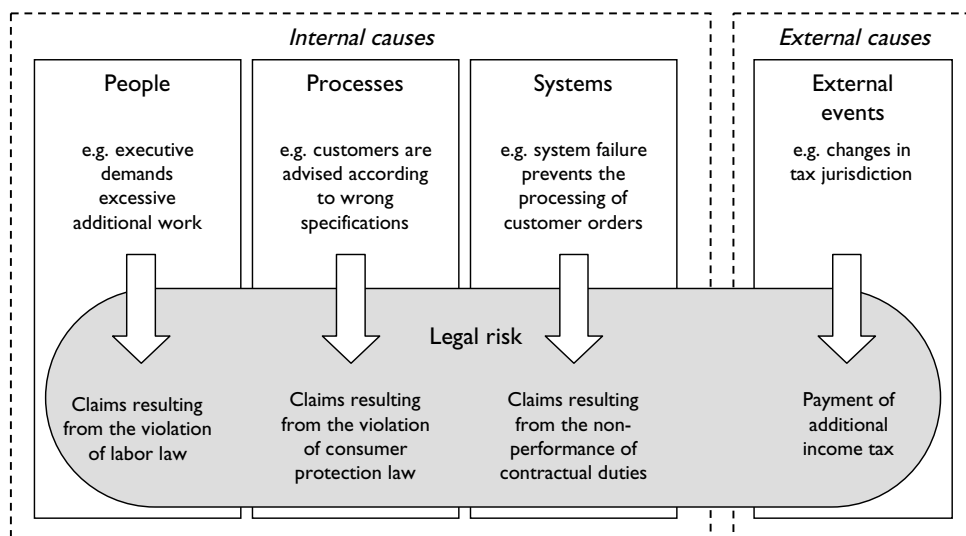


Chart 3.6 Legal Risk as a Horizontal Issue across all Categories of Operational Risk

<sup>80</sup> See [http://www.riskglossary.com/articles/legal\\_risk.htm](http://www.riskglossary.com/articles/legal_risk.htm) (including examples).

<sup>81</sup> Basel Committee on Banking Supervision, Customer Due Diligence for Banks, 2001, p. 4.

Overall, the following important types of legal risk can be identified:

- Risks from **incorrect or imprecise contractual provisions** that lead to adverse effects due to mistakes made in the wording of contracts. Such mistakes may have direct consequences (if, for example, an unlawful clause invalidates the entire contract or an essential part of it) or may entail indirect effects (if, for example, an imprecise wording allows diverse interpretations resulting in a long and risky legal dispute). The latter case has to be given particular consideration in connection with complex contracts, such as outsourcing contracts (see also chapter 2.6.3.2 “Outsourcing”); the risk-mitigating effect of insurances may also be reduced or even fully neutralized by this type of legal risk (see chapter 2.6.3.1 “Insurance”).
- The situation is similar for the risk that claims are unenforceable due to **lacking evidence**, which is typically caused by a process failure or a staff mistake. In most cases, the mistakes relate to the documentation of business transactions (absence of a customer’s signature, lost documents, etc.).
- For quite similar reasons, i.e. shortcomings in business processes or mistakes made by employees, claims may also be unenforceable as they are **barred by time** or due to a **failure to observe time limits**.
- The three risks mentioned above may not only be caused by mistakes made by employees, but also by the **legal counsel** of the credit institution. In that case, however, the liability insurance to be taken out by all Austrian attorneys under Article 21a of the Attorneys Act<sup>82</sup> naturally has to be taken into account. That insurance provides a minimum cover of EUR 400,000 per case for claims resulting from an attorney’s professional activities.
- The risk of losses due to **non-compliance with contractual or legal obligations** may already occur at the process or product level (e.g. a contractually agreed deadline is not met due to excessively complicated processing procedures or a contractual clause is not in line with mandatory legal provisions) or, in individual cases, result from a staff mistake. These cases also show that legal risk extends across the other risk categories and does not constitute an independent form of operational risk; likewise, examples resulting from system-related causes are possible (if the security measures protecting a computer system storing sensitive data are insufficient, this may result in claims for damages and administrative fines under the Data Protection Act).
- The **selective enforceability of claims** relates to cases in which a contract cannot be enforced in its entirety, but only the provisions favourable for one party. The question here is how a legal system allocates the risks to a credit institution and its contract partners. Such situations typically occur in areas in which the legislator considers one party to a contract to need a certain level of protection, i.e. especially under consumer protection and labour law (see also chapter 3.6.2 “Special Legal Risks” below). In those legal fields, special care needs to be taken in drafting and implementing contracts.

<sup>82</sup> Gesetz vom 6. Juli 1868, womit eine Rechtsanwaltsordnung eingeführt wird, Imperial Law Gazette 96/1868, as amended.

- The risk that claims cannot be enforced because a **party lacks the capacity to enter into the contract in question** are not limited to transactions with minors or other persons without full legal capacity (problem of lacking legal capacity). Such risks are also triggered by officers of legal persons acting outside the scope of their powers, agents exceeding the scope of their authorization, trustees acting in breach of good faith, etc.
- Finally, there are legal risks that constitute **external events** since their cause lies outside the credit institution: these include unfavourable changes in the legal situation or jurisdiction (e.g. in consumer protection, taxation or supervisory legislation), unclear or even deficient acts of law or regulations and wrong decisions by authorities.



Chart 3.7: Some Aspects of Legal Risk Forming Part of Operational Risk

### 3.6.2 Special Legal Risks

In each business line of a credit institution, there are special legal risks resulting from the nature of the relevant business activities. Further special legal risks mainly arise from specialized legal provisions. Therefore, the following information is to be seen only as a list of examples illustrating the great variety of legal risks in the individual fields.

In **lending business**, one of the most significant legal risks arises from the field of **collateralization law**. Mistakes made in the establishment of collateral (e.g. missing entry in the land register) or its realization (e.g. failure to observe time limits) may considerably reduce or even destroy the value of collateral. In this context, special problems may arise in cross-border business: foreign legal systems – especially in the CEE countries that are of great interest to Austrian credit institutions – may significantly differ from the Austrian law, for example with regard to the establishment of rights of lien. Furthermore, the issue of enforceability always has to be borne in mind in interna-

tional business. The series of guidelines on credit risk prepared by the OeNB and the FMA contains an in-depth presentation.<sup>83</sup>

Another risk related to credit business results from the use of **securitised products and credit derivatives**. For a detailed discussion of this topic, the readers are also referred to the relevant guidelines published by the OeNB and the FMA.<sup>84</sup>

In trading and treasury, legal risks mainly occur in connection with **derivatives transactions**. In particular in over-the-counter business, complex contractual structures may raise questions that result in considerable clarification efforts in cases of disputes. Additionally, **property-related questions** may be raised in the management of deposited securities and securities transfers; finally, shortcomings in the documentation of transactions could lead to problems in enforcing claims.

Of course, provisions of **banking supervision** law are of major importance, e.g. the relevant requirements of the Austrian Banking Act and applicable special laws. In this context, explicit reference is to be made to regulations to combat money laundering.

In general, **matters covered by special laws** result in special legal risks within their scope and, therefore, need to be given special attention in the fields concerned. Examples are:

- The consumer protection regulations applicable to **contracts with consumers**, notably the Consumer Protection Act<sup>85</sup> as well as bank-relevant special provisions in the Austrian Banking Act<sup>86</sup> and the Act on Distance Marketing of Consumer Financial Services<sup>87</sup>.
- The provisions of **labour law**, including health and safety at work, is a field in which the works council plays a major role because of its information and approval rights as well as its function as the primary contact of employees.
- The provisions of the **Data Protection Act**<sup>88</sup> are particularly important in the IT field (see also the explanations in chapter 3.2.2 “Special Risks – Information Technology”).

A highly special type of legal risk has to be considered in the context of **insurances**, which actually should have the purpose to mitigate operational risk. However, it must not be overlooked that the above explanations on potential difficulties in enforcing claims also apply to insurance contracts. Relatively complex contracts are not seldom, and fuzzy wordings used to define and delimit damage categories and performance obligations may be as problematic as exclusion clauses, exemptions from coverage and similar provisions in the case of disputes. These problems are aggravated especially when events cause

<sup>83</sup> OeNB/FMA, Techniken der Kreditrisikominderung; Leitfäden zum Kreditsicherungsrecht in den 6 CEE-Ländern Kroatien, Polen, Slowakei, Slowenien, Tschechische Republik und Ungarn.

<sup>84</sup> OeNB/FMA, Best Practices in Risk Management for Securitized Products, 2004, p. 27 ff.

<sup>85</sup> Bundesgesetz vom 8. März 1979, mit dem Bestimmungen zum Schutz der Verbraucher getroffen werden, Federal Law Gazette 140/1979, as amended.

<sup>86</sup> Bundesgesetz über das Bankwesen, Federal Law Gazette 532/1993, as amended.

<sup>87</sup> Bundesgesetz über den Fernabsatz von Finanzdienstleistungen an Verbraucher, Federal Law Gazette I 62/2004, as amended.

<sup>88</sup> Bundesgesetz über den Schutz personenbezogener Daten, Federal Law Gazette I No. 165/1999, as amended.

great damage since, in these cases, the survival of a credit institution may depend on prompt payment by the insurance company, while the latter will be highly motivated to reject especially a high claim that is unjustified in its opinion. If the liquidity situation is rather tight, the delay of payment caused by a legal dispute may already suffice to result in serious difficulties for the party insured.

With regard to the specific legal problems arising in the context of **outsourcing**, please see chapter 3.2.2 “Special Risks – Information Technology” and chapter 2.6.3.2 “Outsourcing”.

### 3.6.3 Measures in the Field of Legal Risk

Due to the diverse nature of legal risk, it is difficult to propose general measures to limit this risk. There are, however, certain general principles applying to the response to this risk type.

Legal aspects have to be considered throughout the whole management cycle of operational risks. This principle results from the characteristics of the legal risk as a horizontal matter pervading the other risk categories. Accordingly, measures have to be taken – at the **macro level** – to ensure that the related aspects are considered in every phase of the risk management process (e.g. by raising legal issues during risk analysis or self-assessment). This requires that there is adequate legal expertise which, however, need not necessarily be available in the organizational unit for operational risk management, but may for instance be obtained by involving the legal division or external legal advisors.

In addition, it is necessary to take account of legal risk issues in the overall view at the **micro level** – i.e. within the individual risk categories and business lines. For that purpose, appropriate expert knowledge should be input in those process steps where cases of special legal relevance are dealt with (e.g. conclusion of particularly complex or individually drafted contracts). As a rule, the required knowledge is available in the related organizational units (experts on securities law in trading and settlement, labour law experts in the human resources division, etc.) so that the main task of operational risk managers should be to verify that these aspects have actually been considered or to demand that this is done.

To get informative data for **measuring the legal risk**, it is important not to confine oneself to the collection of legal cases that had a negative impact on the bank’s assets, but to focus on the cause of losses. Therefore, information on those events should be collected and analyzed that eventually triggered the negative legal consequences for the credit institution.<sup>89</sup> This also directly results from the special nature of legal risk.

While it seems hardly possible for a bank to take measures limiting external legal risks taking the form of major changes in the legal system or jurisdiction, it is at least recommendable to reflect on such risks. This is particularly true for markets in which changes of the legal framework are underway. In these cases in which a higher external legal risk is to be expected due to the prevailing situation, reflections on how to address any adverse developments

<sup>89</sup> Wood, Counting the Cost of Legal Risk, 2003.

have to be made at least at a **strategic level** (exit clauses, appropriate selection of the law governing contracts, etc.); if the risk is particularly elevated, specific **business contingency plans** may even be recommendable. Examples of such situations are not limited to countries whose legal system undergoes a transition (e.g. to establish a market economy according to the Western model); the internet – several years ago sometimes still called a “legal vacuum” – was a case in which the rules of the game for a new distribution channel only gradually developed in particular in court rulings, but in part also on the basis of special legal provisions.

Finally, the **involvement of the legal division in day-to-day business** will also make sense in order to mitigate legal risks, especially in fields where an elevated risk has to be expected. Examples are business processes in which complex legal issues have to be addressed so that the expert knowledge available in the specialist division should be supplemented by a separate legal assessment, as well as the development of new products, activities in new business lines or markets (above all, international business). When new processes are established, it is generally necessary to address the question of whether legal aspects could be relevant and, if yes, to consult specialists, the legal division or, if appropriate, also external experts or lawyers depending on the concrete requirements. This is to ensure that the relevant legal requirements are met and that the enforcement of rights does not fail due to unclear or inadequate wordings or due to lacking evidence resulting from insufficient documentation.



## 4 Basel II: Requirements and Capital Standards under Different Approaches

This chapter presents the different approaches for calculating the capital requirements to cover the operational risks of credit institutions. It is based on the proposal for re-casting the European Directive on the capital adequacy of investment firms and credit institutions [2000/12/EC] as accepted by the European Parliament on September 28th 2005<sup>90</sup> and the recommendations of the Basel Committee on Banking Supervision laid down in the revised framework accord “International Convergence of Capital Measurement and Capital Standards” in 2004. Even though the publications of the Basel Committee on Banking Supervision are recommendations without any direct legal effect, it is to be borne in mind that the 1988 Basel capital accord (Basel I) is currently applied by banks of diverse size and complexity in more than 100 countries worldwide.

### 4.1 Introduction

The methods described below strongly differ with regard to their complexity and risk sensitivity and form the basis of calculating the capital requirements for operational risks. As a function of their business lines and the associated risks, banks are requested to move along this spectrum ranging from simple to more complex and more risk-sensitive approaches and further develop their models for measuring and controlling operational risks. In this sense, the different approaches follow an evolutionary design (see chart 4.1<sup>91</sup>).

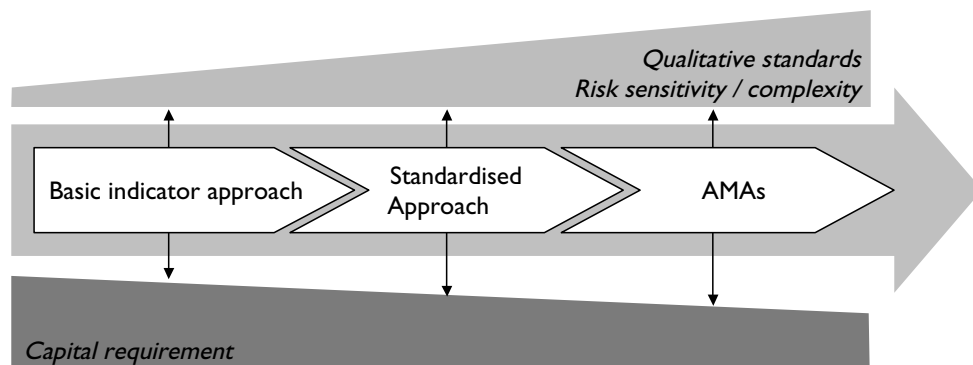


Chart 4.1: Spectrum from Simple to More Risk-Sensitive Approaches

### 4.2 Basic Indicator Approach<sup>92</sup>

#### 4.2.1 General

The basic indicator approach (BIA) is the simplest way of calculating the regulatory capital requirements for a bank's operational risk. It is mainly designed for those banks that, given their size and the complexity of their business, would face unjustifiable efforts if they had to develop and implement more sophisticated approaches.

<sup>90</sup> Meanwhile in effect as directive [2006/48/EC]

<sup>91</sup> Einhaus (2002a), p. 567.

<sup>92</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 1.

In the proposed EU Directive [2000/12/EC], the general risk management standards defined in Article 22 and Annex V have to be complied with when a basic indicator is used to determine the capital requirements for covering operational risks.

#### 4.2.2 Capital Requirement

Under the BIA, the capital requirement for operational risk is equal to 15% of the indicator defined as follows:

The relevant indicator is the average over three years of the sum of net interest income and net non-interest income.

The three-year average is calculated on the basis of the last three twelve-monthly observations at the end of the financial year. When audited figures are not available, estimates may be used. If for any of the three observations, the sum of net interest income and net non-interest income is negative or equal to zero, this figure must not be taken into account in the calculation of the three-year average. The relevant indicator is calculated as the sum of positive figures divided by the number of positive figures.

For credit institutions subject to Directive 86/635/EEC (Directive on the annual accounts and consolidated accounts of banks and other financial institutions), the relevant indicator is expressed as the sum of items 1 to 7 of the profit and loss account of credit institutions pursuant to Article 27 of the Directive. Credit institutions subject to an accounting framework different from the one established by Directive 86/635/EEC calculate the relevant indicator on the basis of data that best reflect the ones listed in the table below.

According to the proposed EU Directive [2000/12/EC] the net interest income and net non-interest income include the following items:

Interest receivable and similar income
Interest payable and similar charges
Income from shares and other variable/fixed-yield securities
Commissions and fees receivable
Commissions and fees payable
Net profit or net loss on financial operations
Other operating income

The following elements shall not be used in the calculation of the indicator:

- realized profits/losses from the sale of non-trading book items,
- income from extraordinary or irregular items, and
- income derived from insurance.

Care is to be taken to ensure that the indicator is calculated before the deduction of any provisions and operating expenses. Operating expenses include fees paid for outsourcing services rendered by third parties which are not a parent or subsidiary of the credit institutions or a subsidiary of a parent which is also the parent of the credit institution. Expenditure on the outsourcing of services rendered by third parties may reduce the indicator if the expen-

diture is incurred by an undertaking subject to supervision under, or equivalent to, the proposed EU Directive [2000/12/EC].

If revaluation of trading book items is part of the profit and loss statement, revaluation could be included in the calculation of the indicator. When Article 36 para. 2<sup>93</sup> of Directive 86/635/EEC is applied, revaluation entered into the profit and loss account should be included.

The formula for calculating the capital requirement under the BIA is:

$$K_{BIA} = \alpha \cdot EI$$

where:

- $K_{BIA}$  = the bank's capital requirement under BIA,
- $\alpha$  = the capital factor (15%), and
- $EI$  = the sum of net interest income and net non-interest income (exposure indicator).

### 4.2.3 Critical Assessment of the Basic Indicator Approach

The BIA is only suitable to a highly limited extent for measuring and controlling operational risks. With a view to its coverage, the operational risk is estimated as a lump sum. Adequate risk management is hardly considered in terms of appropriate risk control because the capital requirement is not determined by the actual operational risks but by the level of net interest income and net non-interest income.

The underlying assumption is that, as a rule, higher income can only be achieved by accepting higher (operational) risks. However, this exclusive attribution to higher operational risks seems only legitimate to a limited extent, because improved performance may also result from better risk management. Altogether, the rough measurement of risks under the BIA hardly provides incentives to a bank for a closer analysis of its operational risks or for improving its risk management.

## 4.3 Standardized Approach<sup>94</sup>

### 4.3.1 General

In comparison with the BIA, the standardized approach is a more advanced method to determine the capital required for covering operational risks. Under this approach, the business activities of a credit institution are subdivided into standardized business lines and assigned a relevant indicator (net interest income and net non-interest income). The capital requirement for operational risks corresponds to the sum of capital requirements in the individual business lines.

The business lines are listed and described in Annex X of the proposed EU Directive [2000/12/EC]:

<sup>93</sup> "The Member States may, however, require or permit those transferable securities to be shown in the balance sheet at the higher market value at the balance sheet date. The difference between the purchase price and the higher market value shall be disclosed in the notes on the accounts." Transposed by Article 56 paragraph 5 of the Austrian Banking Act (*Bankwesengesetz*).

<sup>94</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 2.

Business line	Activities
Corporate finance	Underwriting of financial instruments and/or placing of financial instruments on a firm commitment basis Services related to underwriting Investment advice Advice to undertakings on capital structure, industrial strategy and related matters and advice and services relating to the mergers and the purchase of undertakings Investment research and financial analysis and other forms of general recommendation relating to transactions in financial instruments
Trading and sales	Dealing on own account Money broking Reception and transmission of orders in relation to one or more financial instruments Execution of orders on behalf of clients Placing of financial instruments without a firm commitment basis Operation of Multilateral Trading Facilities
Retail brokerage (activities with individual physical persons or with small and medium-sized entities meeting the criteria for the retail exposure class)	Reception and transmission of orders in relation to one or more financial instruments Execution of orders on behalf of clients Placing of financial instruments without a firm commitment basis
Commercial banking	Acceptance of deposits and other repayable funds Lending Financial leasing Guarantees and commitments
Retail banking (activities with individual physical persons or with small and medium-sized entities meeting the criteria for the retail exposure class)	Acceptance of deposits and other repayable funds Lending Financial leasing Guarantees and commitments
Payment and settlement	Money transmission services Issuing and administering means of payment
Agency services	Safekeeping and administration of financial instruments for the account of clients, including custodianship and related services such as cash/collateral management
Asset management	Portfolio management Managing of UCITS Other forms of asset management

#### 4.3.2 Capital Requirement

The proposed EU Directive [2000/12/EC] defines eight standardized business lines and lays down an indicator for each of them. The capital requirement for a given business line corresponds to a fixed percentage (“beta factor”) of a rel-

evant indicator. This indicator is calculated for each business line individually and equals the average over three years of the sum of net interest income and annual net non-interest income as defined for the BIA.

The three-year average is calculated on the basis of the last three twelve-monthly observations at the end of the financial year. When audited figures are not available, business estimates may be used.<sup>95</sup>

The business lines presented above are assigned different beta factors for which the proposed EU Directive [2000/12/EC] sets out the following values:

• Corporate finance	$\beta_1$	<b>18%</b>
• Trading and sales	$\beta_2$	
• Payment and Settlement	$\beta_6$	
• Commercial banking	$\beta_4$	<b>15%</b>
• Agency services	$\beta_7$	
• Retail brokerage	$\beta_3$	<b>12%</b>
• Retail banking	$\beta_5$	
• Asset management	$\beta_8$	

The capital requirement for operational risk is calculated using the following formula:

$$K_{STA} = \sum_{i=1}^8 K_{STA,i} = \sum_{i=1}^8 \beta_i \cdot EI_i$$

where:

$K_{STA}$  = capital requirement of the institution under the standardized approach

$\sum_{i=1}^8 K_{STA,i}$  = sum of capital requirements in the individual business lines

$\sum_{i=1}^8 \beta_i \cdot EI$  = sum of the products of net interest income and net non-interest income (exposure indicator) for the individual business lines and the beta factors assigned to them

For the treatment of negative values, the proposed EU Directive [2000/12/EC] sets out the following: In each year, a negative capital requirement in one business line, resulting from a negative gross yield, may be imputed to the whole. However, where the aggregate capital charge across all business lines within a given year is negative, the input to the numerator for that year shall be zero.

<sup>95</sup> See proposed EU Directive [2000/12/EC], Annex X, Part, 2 item 5.

### 4.3.3 Business Line Mapping<sup>96</sup>

Both the proposed EU Directive [2000/12/EC] and the New Basel Capital Accord require banks to have principles and documented criteria in place for mapping net interest income and net non-interest income from their own current business lines and activities into the standardized framework. The relevant criteria are reviewed and, if necessary, adjusted to new or changing business activities and risks. The following principles apply to business line mapping:

- *All activities must be mapped into the business lines in a mutually exclusive and jointly exhaustive manner.*
- *Any activity which cannot be readily mapped into the business line framework, but which represents an ancillary function to an activity included in the framework, must be allocated to the business line it supports (e.g. processing of own trading activities). If more than one business line is supported through the ancillary activity, an objective criterion must be used.*
- *If an activity cannot be mapped into a particular business line, then the business line yielding the highest percentage must be used. The same business line equally applies to any associated ancillary activity.*
- *Credit institutions may use internal pricing methods to allocate the relevant indicator between business lines. Costs generated in one business line which are imputable to a different business line may be reallocated to the business line to which they pertain, for instance by using a treatment based on internal transfer costs between the two business lines.*
- *The mapping of activities into business lines for operational risk capital purposes must be consistent with the categories used for credit and market risks.*
- *Senior management is responsible for the mapping policy under the control of the governing bodies of the credit institution.*
- *The mapping process to business lines must be subject to independent review.*

### 4.3.4 Qualifying Criteria

The standardized approach is characterized by a higher level of complexity and risk sensitivity than the BIA.

For applying the standardized approach in the calculation of the capital requirements for operational risks, credit institutions - with regard to the size and scale of their activities and to the principle of proportionality - have to meet the following qualifying criteria as set out in the proposed EU Directive [2000/12/EC]<sup>97</sup> in addition to the general risk management standards defined in Article 22 and Annex V:

1. *Credit institutions shall have a well-documented assessment and management system for operational risk with clear responsibilities assigned for this system. They shall identify their exposures to operational risk and track relevant operational risk data, including material loss data. This system shall be subject to regular independent review.*

<sup>96</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 2, item 8.

<sup>97</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 2, item 17.

2. *The operational risk assessment system must be closely integrated into the risk management process of the credit institution. Its output must be an integral part of the process of monitoring and controlling the credit institution's operational risk profile.*
3. *Credit institutions shall implement a system of management reporting that provides operational risk reports to relevant functions within the credit institution. Credit institutions shall have procedures for taking appropriate action according to the information within the management reports.*

#### **4.3.5 Role of the Competent Supervisory Authorities under the Standardized Approach**

On principle, the proposed EU Directive [2000/12/EC] does not require that the use of the standardized approach is authorized. Nevertheless, it is safe to assume that the competent supervisory authorities will make efforts to obtain a picture of the implementation of the various requirements implied by the standardized approach in the course of their ongoing supervisory activities.

Such an evaluation could comprise the following elements:

- Documentation of the mapping process,
- description of the mapping criteria,
- explanation of the mapping of new types of activities,
- structure of responsibilities and reporting, and
- description of the risk management process for operational risk.

#### **4.3.6 Alternative Standardized Approach<sup>98</sup>**

The alternative standardized approach is a special variant of the standardized approach. Its use by a credit institution needs to be authorized by the supervisory authorities.

##### **4.3.6.1 Specific Conditions**

In addition to the general requirements for applying the standardized approach, the proposed EU Directive [2000/12/EC] specifies the following conditions for the alternative standardized approach:

- *The credit institution is overwhelmingly active in retail and/or commercial banking activities, which shall account for at least 90% of its income.*
- *The credit institution is able to demonstrate to the competent authorities that a significant portion of its retail and/or commercial banking activities comprise loans associated with a high probability of default, and that the alternative standardized approach provides an improved basis for assessing the operational risk.*

##### **4.3.6.2 Modalities**

In contrast to the regular standardized approach, the capital requirement is calculated as follows:

The competent authorities may authorize the credit institution to use an alternative indicator for the business lines of retail banking and commercial banking.

<sup>98</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 2, items 9-16.



For these business lines, the relevant alternative indicator is a normalised volume indicator equal to the three-year average of the total nominal loan volume multiplied by 0.035.

The scope of the two business lines is defined separately in the proposed EU Directive [2000/12/EC].<sup>99</sup>

#### **4.3.7 Critical Assessment of the Standardized Approach and the Alternative Standardized Approach**

Differentiation between business lines is basically a suitable step to raise risk sensitivity in calculating the capital requirement for operational risks. However, the indicator of net interest income and net non-interest income only reflects the business volume in each business line but not the level of operational risk. The capital requirement determined on the basis of these indicators is more risk-sensitive than the one calculated under the BIA, but still its risk adequacy is only limited as bank-specific loss data are not used. Thus, it is difficult to ensure an effective control of operational risks specific to their causes and targeted risk management. Furthermore, potential diversification effects between the business lines are not taken into account by adding up the capital amounts.

With a view to risk measurement, the proposed EU Directive [2000/12/EG] calls for the systematic collection of relevant data on operational risk, including material loss data for each business line. As a result, banks which consider applying the standardized approach should start to build a loss database.

### **4.4 Advanced Measurement Approaches<sup>100</sup>**

#### **4.4.1 General**

The advanced measurement approaches (AMAs) are risk-sensitive methods for measuring operational risk using measurement techniques developed by each individual credit institution. With the explicit authorization of the competent authority, they may be applied from January 1, 2008 at the earliest.

#### **4.4.2 Qualifying Criteria**

##### **4.4.2.1 Qualitative Standards<sup>101</sup>**

In contrast to the two more simple approaches, credit institutions planning to use an advanced measurement approach have to meet additional qualitative standards. These are defined in the proposed EU Directive [2000/12/EC] as follows:

- *The credit institution's internal operational risk measurement system shall be closely integrated into its day-to-day risk management processes.*
- *The credit institution must have an independent risk management function for operational risk.*

<sup>99</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 2, item 11.

<sup>100</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 3.

<sup>101</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 3, item 1.

- *There must be regular reporting of operational risk exposures and loss experience. The credit institution shall have procedures for taking appropriate corrective action.*
- *The credit institution's risk management system must be well documented. The credit institution shall have routines in place for ensuring compliance and policies for the treatment of non-compliance.*
- *The operational risk management processes and measurement systems shall be subject to regular reviews performed by internal and/or external auditors.*
- *The validation of the operational risk measurement system by the competent authorities shall include the following elements:*
  - *Verifying that the internal validation processes are operating in a satisfactory manner;*
  - *Making sure that data flows and processes associated with the risk measurement system are transparent and accessible.*

The binding qualitative standards described in the proposed EU Directive [2000/12/EC] are covered in somewhat greater detail in the “New Basel Capital Accord”. These may, therefore, constitute a useful complement to the requirements specified in the directive.<sup>102</sup>

#### 4.4.2.2 Quantitative Standards<sup>103</sup>

In addition to the qualitative standards to be met by operational risk processes and management, the credit institutions also have to observe and comply with quantitative requirements.

When selecting and developing a suitable method, the bank has to be able to prove that the measurement method it selected and developed is capable of capturing potentially severe tail events. The capital requirement is calculated as comprising both expected loss and unexpected loss, unless the credit institution can demonstrate that expected loss is already adequately captured in internal business practices. Irrespective of the approach selected, the bank has to prove that the operational risk measure achieves a soundness standard comparable to a 99.9% confidence interval over a one year period.

According to the proposed EU Directive [2000/12/EC], the operational risk measurement system must have the following key elements to meet the soundness standard mentioned above:

- internal data,
- external data,
- scenario analyses and
- factors reflecting the business environment and internal control systems.

The credit institution needs to have a well-documented approach for weighting the use of these four elements in its measurement system.<sup>104</sup>

Correlations in operational risk losses across individual operational risk estimates may be recognized only if credit institutions can demonstrate to the satisfaction of the competent supervisory authorities that the system they use for measuring correlations is sound and sufficiently takes into account the

<sup>102</sup> See Basel Committee on Banking Supervision, The New Basel Capital Accord, paragraph 666.

<sup>103</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 3, items 8-12.

<sup>104</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 3, item 9.

uncertainty surrounding any such correlation estimates, particularly in periods of stress. The correlation assumptions must be validated using appropriate quantitative and qualitative techniques.<sup>105</sup>

The risk measurement system must be internally consistent. The multiple counting of qualitative assessments or risk mitigation techniques already recognized in other areas of the capital adequacy framework must be avoided.<sup>106</sup>

#### 4.4.2.3 Treatment of Internal Data<sup>107</sup>

Internally generated operational risk measures used for regulatory capital calculation must be based on a minimum historical observation period of five years for internal loss data. When a credit institution first moves to an AMA, a three-year data series is acceptable according to the proposed EU Directive [2000/12/EC].<sup>108</sup>

The proposed EU Directive [2000/12/EC] defines the following requirements for the collection of internal loss data to be met by banks:<sup>109</sup>

- *The credit institution's internal loss data must be comprehensive in that it captures all material activities and exposures from all appropriate subsystems and geographic locations. Credit institutions must be able to justify that any excluded activities or exposures, both individually and in combination, would not have a material impact on the overall risk estimates. Appropriate minimum loss thresholds for internal loss data collection must be defined.*
- *Aside from information on gross loss amounts, credit institutions shall collect information about the date of the event, any recoveries of gross loss amounts, as well as some descriptive information about the drivers or causes of the loss event.*
- *There shall be specific criteria for assigning loss data arising from an event in a centralized function or an activity that spans more than one business line, as well as from related events over time.*
- *Credit institutions must have documented procedures for assessing the ongoing relevance of historical loss data, including those situations in which judgement overrides, scaling, or other adjustments may be used, to what extent they may be used and who is authorized to make such decisions.*

To ensure that supervisory authorities recognize a loss database, historical internal loss data are mapped into the business lines defined for the standardized approach and into the event-type categories laid down (see Annex). At any rate, information is to be recorded on the level of losses, date of loss events, indemnification received and causes of loss events. Moreover, cases of loss are frequently based on several operational loss events that may mutually reinforce each other. They may also be caused by more than one type of risk.

As it is difficult to differentiate between credit risk and operational risk, the following solution was adopted in the proposed EU Directive [2000/12/EC]: The operational risk losses that are related to credit risk and have historically been included in the credit risk database continue to be treated as credit

<sup>105</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 3, item 11.

<sup>106</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 3, item 12.

<sup>107</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 3, item 13-18. See also chapter 2.5.2.1 "Internal Loss Databases".

<sup>108</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 3, item 13.

<sup>109</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 3, items 15-18.

risk for calculation purposes. To avoid duplication, such losses will not be subject to the operational risk charge. However, credit institutions must keep records of all operational losses for the purposes of internal loss data collection. As a result, losses related to credit risks are to be separately identified in the operational risk databases.

#### 4.4.2.4 Treatment of External Data<sup>110</sup>

When a bank applies an AMA, the operational risk management system has to use relevant external data according to the proposed EU Directive [2000/12/EC]. These external data may include public data and/or data exchanged among banks. External data are required especially when there is reason to believe that the bank is exposed to infrequent, yet potentially severe, losses. For this purpose, the bank must have a systematic process to determine the situations for which external data must be used and to define the methodologies applied to process these data. The conditions and practices for using external data must be regularly reviewed, documented and subject to periodic independent review.

#### 4.4.2.5 Scenario Analysis<sup>111</sup>

A bank applying an AMA has to perform scenario analyses on the basis of expert opinion in conjunction with external data to evaluate its exposure to high severity events for which insufficient internal data are available. In this process, experienced managers and risk management experts provide their inputs so that assessments are obtained on potentially severe losses. These assessments can be expressed as parameters of an assumed statistical loss distribution.

The proposed EU Directive [2000/12/EC] requires that these assessments be validated over time and appropriately adjusted through comparisons with actual loss experience to ensure their reasonableness.

#### 4.4.2.6 Business Environment and Internal Control Factors

In addition to internal and external loss data as well as scenario analyses, the business environment and internal control factors are a key element of AMAs. For this reason, the proposed EU Directive [2000/12/EC] provides that the bank's firm-wide risk assessment system must capture key business environment and internal control factors that can influence its operational risk profile. As a result, the bank's risk assessment becomes more future-oriented and better reflects the quality of controls and the immediate business environment. This can make a significant contribution to better coordinate capital requirements and risk management objectives and recognize both improvements and deteriorations of the operational risk profile earlier.

<sup>110</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 3, item 19. See also chapter 2.5.2.2 "External Loss Databases".

<sup>111</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 3, item 20. See also chapter 2.5.4 "Scenario Analysis".

When these factors are used in the bank's risk measurement framework, several supervisory requirements have to be met. In this context, the proposed EU Directive [2000/12/EC] stipulates:<sup>112</sup>

- *The choice of each factor needs to be justified as a meaningful driver of risk, based on experience and involving the expert judgment of the affected business areas.*
- *The sensitivity of risk estimates to changes in the factors and the relative weighting of the various factors need to be well reasoned. In addition to capturing changes in risk due to improvements in risk controls, the framework must also capture potential increases in risk due to greater complexity of activities or increased business volume.*
- *This framework must be documented and subject to independent review within the credit institution and by competent authorities. Over time, the process and the outcomes need to be validated and reassessed through comparison to actual internal loss experience and relevant external data.*

#### **4.4.3 Recognition of the Risk-Mitigating Impact of Insurance and other Risk Transfer Mechanisms<sup>113</sup>**

The proposed EU Directive [2000/12/EC] recognizes the impact of insurance and other risk transfer mechanisms where the credit institution can demonstrate to the satisfaction of the competent authority that a noticeable risk mitigation is achieved. This recognition, however, is limited to 20% of the overall capital requirement for operational risks and is subject to the following conditions:

- *The provider is authorized to provide insurance or re-insurance.*
- *The provider has a minimum claims paying ability rating by an eligible ECAI which has been determined by the Financial Market Authority (FMA) to be associated with credit quality step 3 or above under the rules for the risk weighting of exposures to credit institutions according to the Standardized Approach<sup>114</sup>.*
  - *The insurance policy must have an initial term of no less than one year. For policies with a residual term of less than one year, the credit institution must make appropriate haircuts reflecting the declining residual term of the policy, up to a full 100% haircut for policies with a residual term of 90 days or less.*
  - *The insurance policy has a minimum notice period for cancellation of the contract of 90 days.*
  - *The insurance policy has no exclusions or limitations triggered by supervisory actions or, in the case of a failed credit institution, that preclude the credit institution, receiver or liquidator from recovering for damages suffered or expenses incurred by the credit institution, except in respect of events occurring after the initiation of receivership or liquidation proceedings in respect of the credit institution, provided that the insurance policy may exclude any fine, penalty, or punitive damages resulting from actions by the competent authorities.*
  - *The risk mitigation calculations must reflect the insurance coverage in a manner that is transparent in its relationship to, and consistent with, the actual likeli-*

<sup>112</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 3, items 22-24.

<sup>113</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 3, items 25-29.

<sup>114</sup> See proposed EU Directive [2000/12/EC], Articles 78 to 83.

*hood and impact of loss used in the overall determination of operational risk capital.*

- *The insurance is provided by a third party entity. In the case of insurance through captives and affiliates, the exposure has to be laid off to an independent third party entity, for example through reinsurance that meets the eligibility criteria.*
- *The framework for recognizing insurance is well reasoned and documented.*
- *The methodology for recognizing insurance shall capture the following elements through discounts or haircuts in the amount of insurance recognition:*
  - *The residual term of a policy, where less than one year, as noted above;*
  - *A policy's cancellation terms, where less than one year;*
  - *The uncertainty of payment as well as mismatches in coverage of insurance policies.*

#### **4.4.4 Application of an AMA on a Group-Wide Basis**

When an EU parent credit institution or an EU parent financial holding company and their subsidiaries intend to use an AMA, this group-wide model must be authorized by the competent authority having jurisdiction at the registered office of the parent company according to the proposed EU Directive [2000/12/EG].<sup>115</sup> The application to use a group-wide model should give special consideration to the description of the methodology used for allocating operational risk capital to the group's subsidiaries. The description should also indicate whether and how diversification effects are to be factored in the risk measurement system.<sup>116</sup>

#### **4.4.5 Authorization of an AMA by Competent Authorities**

The proposed EU Directive [2000/12/EC] explicitly provides that the use of an AMA needs to be authorized by the competent authority.<sup>117</sup>

In the application procedure, credit institutions have to submit, among others, the following documents:

- detailed roll-out plan,
- documentation and description of the AMA model,
- information on partial use,
- description of the model parameters,
- IT implementation of the AMA model,
- structure of responsibilities and reporting,
- description of the risk management process for operational risk, and
- information on employee training.

<sup>115</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 3, items 30-31.

<sup>116</sup> For further information on the use of an AMA on a group-wide basis, see the consultation paper "CEBS Guidelines on the Implementation, Validation and Assessment of Advanced Measurement (AMA) and Internal Ratings Based (IRB) Approaches" (<http://www.c-ebs.org>).

<sup>117</sup> For further information on the authorization of an AMA, see the consultation paper "CEBS Guidelines on the Implementation, Validation and Assessment of Advanced Measurement (AMA) and Internal Ratings Based (IRB) Approaches" (<http://www.c-ebs.org>).



#### 4.4.6 Partial Use of Different Operational Risk Approaches<sup>118</sup>

On principle, the partial use of two different measurement approaches is only permitted in combination with an AMA. If a bank decides to apply an AMA, this approach may be combined with either the basic indicator approach (BIA) or the standardized approach. Special requirements to be met in the case of partial use are:

- All operational risks of the credit institution are captured. The competent authority shall be satisfied with the methodology used to cover different activities, geographical locations, legal structures or other relevant divisions determined on an internal basis.
- The qualifying criteria are fulfilled for the part of activities covered by the standardized approach and AMAs respectively.

On a case-by-case basis, the supervisory authority may impose the following additional conditions:

- *On the date of implementation of an AMA, a significant part of the credit institution's operational risks are captured by the AMA.*
- *The credit institution takes a commitment to roll out the AMA across a material part of its operations within a time schedule agreed with its competent authorities.*

The BIA and the standardized approach may only be combined in exceptional circumstances and for a limited period of time. According to the directive, such exceptional circumstances may be the recent acquisition of new business which may require a transition period agreed with the competent authority for the roll out of the standardized approach all over the company.<sup>119</sup>

#### 4.4.7 Critical Assessment of AMAs

As AMAs take better account of the banks' individual experiences with operational risks and the causes of such risks, they are basically more risk-sensitive and risk-adequate than simpler approaches. When using these methods, credit institutions need to actively deal with their operational risks in regular analyses and assessments so that advanced methods may be excellently suited to risk control and risk management and can be used within the framework of internal and bank-wide capital allocation.

An AMA may, on principle, lead to a reduction of the capital required for covering operational risks. This is, however, limited by the provisions of Article 152 of the proposed EU Directive [2000/12/EC].

### 4.5 Capital Requirements for Covering the Operational Risk of Investment Firms

Due to the recast of EU Directive [2000/12/EC], Directive [93/6/EEC] (Capital Adequacy Directive – CAD) is also amended. It lays down in Article 20 (3) and Article 21, that investment firms which are not allowed to hold money or securities of customers, have to provide own funds corresponding to the minimum starting capital or to 25% of the company's fixed overheads, whichever

<sup>118</sup> See proposed EU Directive [2000/12/EC], Annex X, Part 4.

<sup>119</sup> For further information on partial use, see the consultation paper "CEBS Guidelines on the Implementation, Validation and Assessment of Advanced Measurement (AMA) and Internal Ratings Based (IRB) Approaches" (<http://www.c-ebs.org>).



amount is higher, in order to meet the capital requirement for covering operational risks. The level of the fixed overheads is to be determined on the basis of the previous audited annual financial statement. These provisions largely correspond to the current situation laid down in Article 22, paragraph 2 of the Austrian Securities Supervision Act (Wertpapieraufsichtsgesetz) and, as a result, do not lead to significant changes for investment firms that, under Austrian law, are referred to as investment service providers in the Securities Supervision Act.

Under Article 20, paragraph 2, item 1 of the Austrian Securities Supervision Act, the minimum starting capital of investment service providers must equal EUR 50,000 provided that their business purpose exclusively includes investment advice regarding customers' funds (Article 1, paragraph 1, item 19, lit. a of the Austrian Banking Act) and/or the mediation of business opportunities for the sale and purchase of one of the instruments mentioned in Article 1, paragraph 1, item 7, lit. b to f of the Austrian Banking Act (Article 1, paragraph 1, item 19, lit. c of the Austrian Banking Act), or EUR 125,000 provided that their business purpose extends to the management of customer portfolios including power of disposal on behalf of the customer (Article 1, paragraph 1, item 19, lit. b of the Austrian Banking Act).

Due to the legal requirements defined in Article 22, paragraph 2 of the Austrian Securities Supervision Act and the resulting methods for calculating the minimum capital always to be held, the capital requirement of investment service providers may also exceed the minimum starting capital of EUR 50,000 or EUR 125,000 because their minimum capital always has to equal at least 25% of the fixed overheads of the previous audited annual financial statement.

Pursuant to Article 22, paragraph 2 of the Austrian Securities Supervision Act, fixed overheads include the operating expenses that are independent of the investment service provider's level of activity and that are not directly allocated to the individual cost units (products). Fixed overheads are calculated from the operating expenditure specified in the layout defined in Annex 2 to Article 43, part 2 of the Austrian Banking Act as follows:

- Personnel expenditure: primarily reduced to the expenditure incurred by executives and senior employees;<sup>120</sup>
- Other administrative expenditure (overhead): with regard to operating costs of motor vehicles as well as telephone, postage and representation costs, costs directly attributable to individual cost units are to be deducted on principle; operating costs of premises and offices, legal, audit and consultancy fees as well as any fees paid to members of the supervisory board and license fees are to be included without any deductions;
- Value adjustments of the fixed assets and tangible assets as well as other operating expenditure shall be fully included in the fixed overheads.

The national transposition of the proposed EU Directive [2000/12/EC] in its final version is unlikely to result in significant changes to the mandatory shareholders' equity of investment service providers on account of capital requirements for covering operational risks. Please note, however, that the forthcom-

<sup>120</sup> See Frölichsthal, p. 207.

ing national transposition of Directive 2004/39/EC (Markets in Financial Instruments Directive – MiFID) and other European legislative projects may involve changes in the scope of business of Austrian investment service providers and, as a result, may have an impact on their equity basis. Overall, the new developments brought about by Basel II and the transposition of the MiFID into national law require investment service providers to rethink and raise their awareness of operational risks.

## References

- Bank of England**, Report of the board of banking supervision inquiry into the circumstances of the collapse of Barings, 1995, cited from: <http://www.numa.com/ref/barings/bar00.htm>
- Basel Committee on Banking Supervision**, International Convergence of Capital Measurement and Capital Standards, BIS, 2004.
- Basel Committee on Banking Supervision**, Customer Due Diligence for Banks, BIS, 2001.
- Basel Committee on Banking Supervision**, Sound Practices for the Management and Supervision of Operational Risk, BIS, 2003.
- Basel Committee on Banking Supervision**, A New Capital Adequacy Framework: Consultative Document, 1999.
- Basel Committee on Banking Supervision**, Consultative Document: Operational Risk, 2001.
- Basel Committee on Banking Supervision**, Framework for Internal Control Systems in Banking Organizations, 1998.
- Bundesamt für Sicherheit in der Informationstechnik**, IT-Grundschutzhandbuch, 2004, available from: <http://www.bsi.de/gshb/deutsch/index.htm>
- CEBS**, The High Level Principles on Outsourcing, Consultative Paper, 2004, available from: [http://www.c-ebs.org/Consultation\\_papers/CP02.htm](http://www.c-ebs.org/Consultation_papers/CP02.htm)
- Chini/Frölichsthal**, Praxiskommentar zum Bankwesengesetz, 2. Aufl., Ueberreuter, Wien 1997.
- COSO**, Internal Control – Integrated Framework, 1992.
- Cruz (Ed.)**, Operational Risk Modelling and Analysis, Risk Books, London 2004
- Digenan/Felson/Kelley/Wiemert**, Metallgesellschaft AG: A Case Study, cited from: <http://www.stuart.iit.edu/fmtreview/fmtrev3.htm>
- Eller/Gruber/Reif (Hrsg.)**, Handbuch Operationelle Risiken, Schäffer-Poeschel Verlag, Stuttgart 2002.
- Einhaus**, Operationelle Risiken in Kreditinstituten, in: Die Sparkasse, Nr. 119, Ausgabe 12, Dezember 2002, 566ff.
- Ernst & Young**, Studie: Wirtschaftskriminalität in Deutschland – Nur ein Problem der anderen?, 2003, available from: [http://www.ey.com/global/download.nsf/Austria/wirtschaftskriminalitaet/\\$file/Wirtschaftskriminalitaet.pdf](http://www.ey.com/global/download.nsf/Austria/wirtschaftskriminalitaet/$file/Wirtschaftskriminalitaet.pdf)
- Franke**, Mitarbeiterkriminalität – Der Feind in den eigenen Reihen, in: Die Bank 9/2004, 76ff.
- Hofmann**, Identifizierung, Quantifizierung und Steuerung operationeller Risiken in Kreditinstituten, Bankakademie Verlag, Frankfurt 2002.
- IAEA**, The Chernobyl Accident, Safety Series No. 75 – INSAG-7, Vienna 1992.
- ISDA**, Operational Risk Regulatory Approach – Discussion Paper, published on <http://www.isda.org/press/pdf/orradp900.pdf>
- ITWG**, Industry Technical Working Group on Operational Risk, 2003.
- Joint Forum**, Operational Risk Transfer across Financial Sectors, BIS, 2003.
- Joint Forum**, Outsourcing in Financial Services, BIS, 2005.
- Jorion**, Big Bets Gone Bad: Derivatives and Bankruptcy in Orange County, Academic Press, 1995.
- Jörg**, Operational Risk – Herausforderung bei der Implementierung von Basel II, Bankakademie Verlag, 2003
- Kraft/Balduin**, Der Mensch ist Mensch – weil er Fehler macht und weil er irrt: Risikofaktor Mitarbeiter, in: Risknews 9/2002, 29ff.
- Kreische/Bretz**, Anforderungen an die Informationstechnologie der Kreditinstitute, in: Die Bank 5/2003, 321ff.
- Kuratorium für Verkehrssicherheit**, Unfallstatistik 2003, 2004.
- Minz**, Operationelle Risiken in Kreditinstituten, Bankakademie Verlag, 2002
- Münchener Rückversicherungs-Gesellschaft**, World of Natural Hazards, 2000.
- OeNB/FMA**, Best Practices in Risk Management for Securitized Products, 2004.
- OeNB/FMA**, Credit Approval Process and Credit Risk Management, 2004.
- OeNB/FMA**, Guidelines on “Bank-Wide Risk Management”, 2005
- OeNB/FMA**, Guidelines on Credit Risk Mitigation: Legal Framework in Croatia, Poland, Slovakia, Slovenia, the Czech Republic and Hungary, 2004.
- OeNB/FMA**, Rating Models and Validation, 2004.

- OeNB/FMA**, Techniken der Kreditrisikominderung, 2004.
- Österreichisches IT-Sicherheitshandbuch**, Version 2.2, 2004, available from <http://www.cio.gv.at/securenetworks/sihb/>
- Power**, The Invention of Operational Risk, ESRC Discussion Paper No. 16, available from <http://www.lse.ac.uk/collections/CARR/pdf/Disspaper16.pdf>
- PwC**, Investigation into foreign exchange losses at the National Australia Bank, 2004.
- n.n.**, Risky Stars – Ein Interview mit Rainer Bäcker, in: Risknews 9/2002, 13ff.
- Romeike**, IT-Risiken und Grenzen traditioneller Risikofinanzierungsprodukte, in: Zeitschrift für Versicherungswesen, Nr. 51, Ausgabe 17, September 2000, 603ff.
- Romeike**, Risikomanagement jenseits der exakten statistisch-mathematischen Methoden – Erst kommt das Fressen, dann kommt die Moral, in: Risknews 9/2002, 6ff.
- Roßbach/Locarek-Junge (Hrsg.)**, IT-Sicherheitsmanagement in Banken, Bankakademie-Verlag, Frankfurt am Main, 2002
- Utz**, Bedeutung operationeller Risiken aus Sicht von Banken und Sparkassen, in: Eller/ Gruber/Reif (Hrsg.) Handbuch Operationelle Risiken, Schäffer-Poeschel Verlag, Stuttgart 2002.
- van den Brink**, Operational Risk – Wie Banken das Betriebsrisiko beherrschen, Schäffer-Poeschel Verlag, Stuttgart 2001.
- von Heyden**, Mitarbeiterkriminalität – Umfeld und Hintergründe, in: Die Bank 4/1999, 228 ff.
- Verstaen**, Business Continuity – Wie viel Hochverfügbarkeit braucht ein Unternehmen, in: Risknews 9–12/2003, 34ff.
- Wood**, Counting the Cost of Legal Risk, 2003, cited from: <http://www.erisk.com/ResourceCenter/Operational/CountingTheCostofLegalRis.asp>

## Annex

### Categories of operational loss events

Event-type category	Description
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one internal party.
External fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.
Employment practices and workplace safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/discrimination events.
Clients, products and business practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.
Damage to physical assets	Losses arising from loss or damage to physical assets from natural disaster or other events.
Business disruption and system failures	Losses arising from disruption of business or system failures.
Execution, delivery and process management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors.