# Scenario-based AMA

**May 2003, Final Version 1.0**

Banca Intesa
Barclays Bank
Credit Suisse First Boston
Dresdner Bank
Fortis Bank
Halifax Bank of Scotland
Lloyds TSB
The Royal Bank of Scotland Group
UFJ Holdings Inc
Euroclear

*The named banks have contributed to the content and drafting of this paper. Such contributions do not imply that the institutions will implement the approach set out in the paper, but rather that they believe a Scenario-based AMA is conceptually sound and, if implemented with integrity, should be recognised as qualifying for AMA status. The views expressed do not necessarily reflect the overall view of each individual institution.*

## Abstract

The scenario-based AMA (sbAMA) working group, a group of internationally active banks coordinated by Dresdner Bank, has focused on an AMA model, which is based on a forward looking assessment of the operational risks an organisation is exposed to.

This paper describes the key features and the main steps in the process of a sbAMA. It aims to demonstrate that the methodology outlined is a conceptually sound and valuable basis for managing and measuring risks, while at the same time addressing the regulatory requirements for an AMA as defined in the current Basel 2 proposals.

Moreover, the paper reflects the intellectual alignment of participating institutions in terms of their thinking about scenarios as well as showing how the latter can form an integral part of economic and regulatory capital calculations.

The working group believes that historical data alone cannot be sufficiently indicative of an organisation's operational risk. The complex underlying and dynamic causes of operational risk necessitate a progressive and proactive approach to risk management, drawing on all available information such as expert experience, internal and relevant external loss histories as well as key operational risk indicators and the quality of the control environment.

By placing scenarios at its centre, a sbAMA enables all of these elements to influence both the capital calculation and operational risk management decisions. It creates a forward-looking risk management framework that provides a direct link to business specific management actions and is responsive to changes in both the internal and external environment.

The involvement of key stakeholders in the scenario generation and evaluation cycle creates risk awareness and supports the identification of management priorities.

## Table of Contents

# 1 Principles and application of the sbAMA

## 1.1 Principles

Risk, defined as the combination of severity and frequency of potential loss over a given time horizon, is inextricably linked to the evaluation of scenarios. Scenarios are potential future events. Their evaluation involves answering two fundamental questions: firstly, what is the potential frequency of a particular scenario occurring and secondly, what is its potential loss severity?

In order to assess exposure to a certain risk type (such as market, credit or operational risk) it is necessary to determine a representative set of scenarios, that reflects the drivers of the risk type in question. In market risk such scenarios are typically based on changes in financial markets, e.g., a yield curve shift by 20bp, and in credit risk on changes in creditworthiness, e.g., a default or downgrading of a certain customer.

Turning to operational risk, it is necessary for a firm to follow a clear procedure when generating a representative set of scenarios that takes into account all relevant drivers of risk (referred to herein as risk factors). A business depends on such risk factors (people, IT, controls), and is vulnerable if they fail, deteriorate or are of poor quality. The evaluation of risk should focus on such vulnerabilities and should have regard to changes in the quality of risk factors, which can be evaluated in a number of dimensions (e.g. high/medium/low, red/amber/green traffic lights, scores out of ten, percentages etc).

Risk factors can usually be categorized and thus give rise to scenario classes (e.g. IT breakdown). To derive scenarios from each of the scenario classes that are specific to a particular organisational part (e.g. Retail Banking), some form of organisational mapping (whether by product, process or business unit) is required. For each combination of scenario class and organisational part scenarios will then be designed in the form of "what-if" questions.

The process of answering the "what-if"-questions is risk assessment (the process is referred to as self-assessment when undertaken by the risk takers themselves). In accordance with the definition of risk it must lead to an evaluation of the potential loss frequency and severity of financial impact of particular scenarios. The assessment takes account of all available information such as expert experience, key risk indicators, the quality of risk factors, historical internal data, and relevant external loss events. The weighting attributed to each depends on the quality of the information available and the degree of change faced by the business.

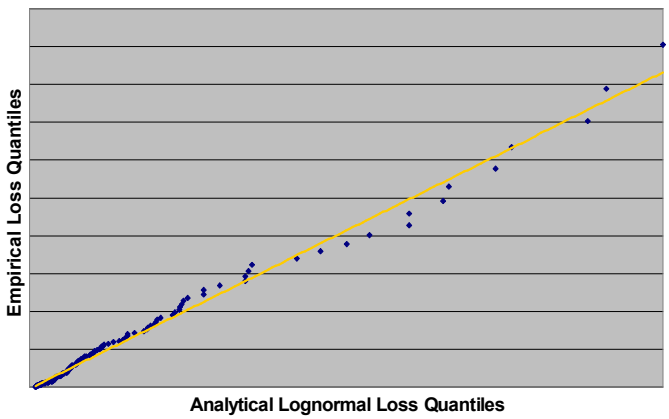



*Figure 1: Plot of empirical quantiles of OR losses and theoretical quantiles of a lognormal distribution*

The objective of a risk assessment is to understand the level of operational risk in a defined part of the organisation, with the results being reported to enable better-informed risk management decisions to be taken. For example, where underlying risk factors are assessed as being of poor quality, risk can be reduced by improving their quality.

In order to determine an overall risk capital number that is justifiable, it is necessary to have a robust and consistent risk model that has been designed and built to be stable over time. This ensures that changes in economic or regulatory capital are driven by alterations of the underlying risk profile and not by variations in the risk model. The model must be defined in terms of a function that relates the required input parameters to the resulting risk capital number. A good risk model should therefore also take account of the diversification effect

across scenario classes and organisational parts, i.e., not all the losses from exposures identified in the scenario assessment occur simultaneously.

It is obvious that any distributional assumptions in the risk model need to be credible. This can for instance be achieved by statistical analysis such as qq-plots like that shown in figure 1. Examples of distributions used include lognormal, normal gamma, Gumbel, Weibull, or Frechet to model loss severities and (negative) binomial or Poisson for loss frequencies.

## 1.2 Application of sbAMA

The sbAMA is considered to be conceptually sound on the basis that information is only fed into a capital computation model if it is relevant to the operational risk profile of an organisational part and thus is needed to answer the "what-if" questions in the scenario assessment. Furthermore the overall sbAMA process must be supported by a sound and structured organisational OR framework and by an adequate IT infrastructure. The sbAMA comprises six main steps, which are illustrated in figure 2 below and will be individually described in the following subsections.

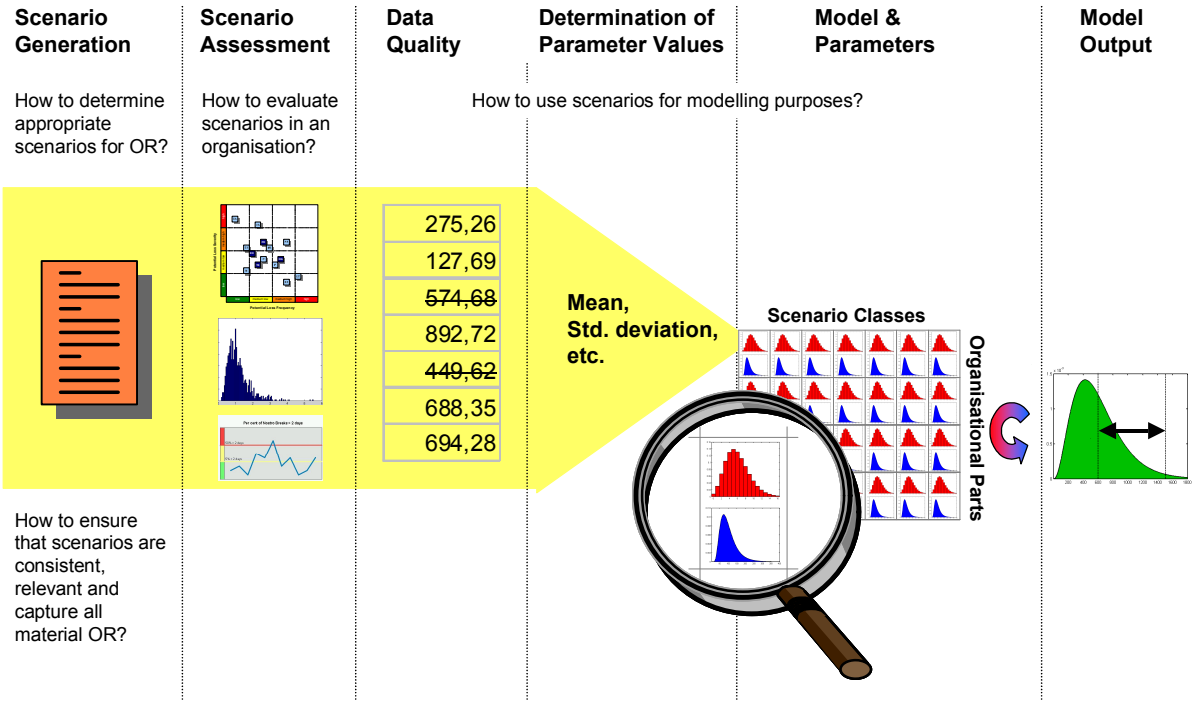



*Figure 2: Overview of the sbAMA*

### 1.2.1 Scenario Generation

Scenario generation represents the first step of the sbAMA. The aim is to determine scenarios which capture all material risks, can be applied consistently across the company and are relevant to specific organisational parts. This is achieved by following a clearly documented procedure involving a sequence of key steps.

Firstly, all risk factors reflecting the operational risk profile (i.e. vulnerabilities of the organisation) are identified from the experience of experts using a number of techniques such as facilitated workshops and questionnaires. These risk factors can be categorised into scenario classes.

Secondly, this common set of scenario classes is applied to differing organisational parts thereby ensuring consistency across the whole organisation, even though the individual scenarios per class will differ due to the different vulnerabilities per organisational part (e.g. different IT-systems).

Thirdly, on the basis of the scenario classes, business experts determine the individual scenarios that are relevant for the organisational part that is assessing its operational risk (e.g. if an organisational part is not vulnerable to IT failure, it does not make sense to evaluate the risk of a break-down of its particular IT-system). They do this

based on their business knowledge, experience and expectations, while referring to relevant loss data and the full range of loss types to ensure that the scenarios identified are comprehensive as well as relevant. Here again,

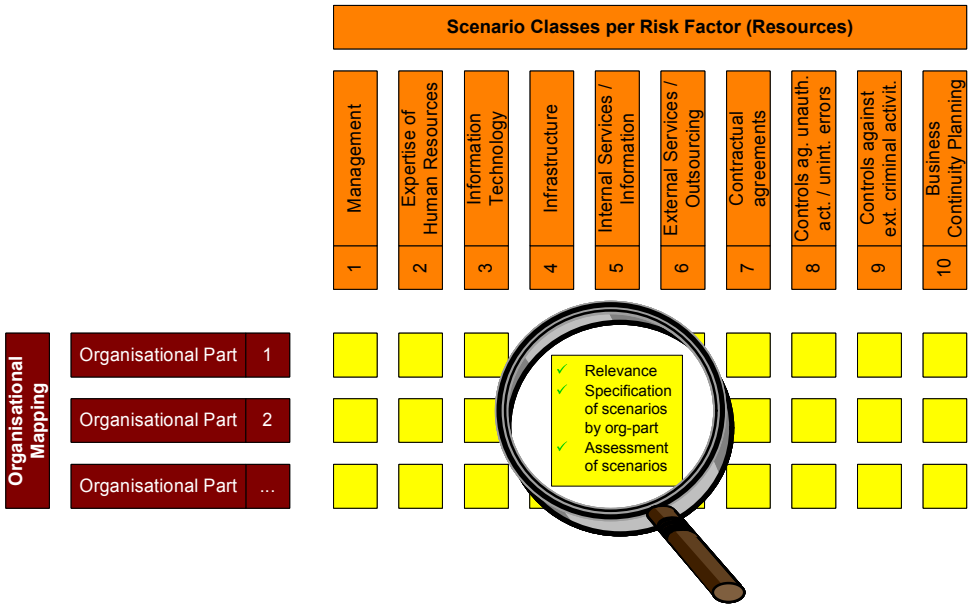



*Figure 3: Scenario documentation*

techniques such as guided discussions in workshops are used to steer the scenario identification in the right direction. For the purposes of the assessment these scenarios should be documented. An example is visualised in figure 3.

### 1.2.2 Scenario Assessment

The second step of the sbAMA involves the assessment of the generated scenarios. This is achieved through managerial expertise based on a blend of information such as historical losses, key risk indicators, insurance cover, the quality of relevant risk factors and the control environment, as well as relevant industry experience. The balance of the individual elements in the blend depends on the amount, and quality of historical data available and its relevance to the current scenario assessment, given the extent of internal and external change facing the business.

It is important to note that the "what-if"question in the scenario drives which data should be used. For instance, the use of historical data may be preferred for evaluating the potential frequency of a particular scenario, where good quality data is available and the level of change is minimal.

Where insufficient historical data is available, experts must estimate the potential loss frequency and severity for a specific scenario, given their experience and business knowledge. Similar to the process for scenario generation, the assessment is undertaken in the form of guided discussions or formalised questionnaires to ensure comprehensiveness and consistency.

Frequency and severity estimates should reflect typical and upper bound values (see figure 4). In order to achieve credible results, scenario assessment requires clear definitions and guidelines enshrined in a standardised process, appropriate training and independent challenge of the experts' estimates. Furthermore, it is key that the assessment is based on a clear view of the business area activities or processes and that corresponding data sources are available.

### 1.2.3 Data Quality

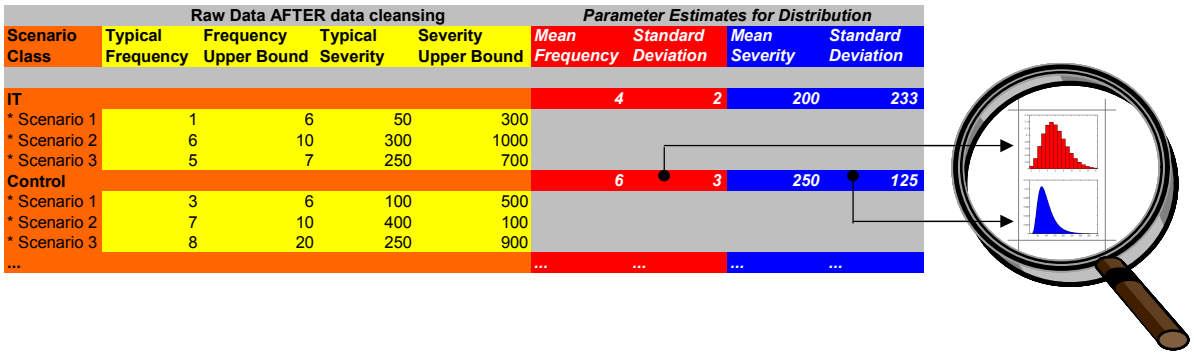
Once the scenario assessment is completed the validity of the results must be ensured. Therefore, the third step of the sbAMA ensures that the resulting data from the scenario assessment (which will subsequently be used for risk capital modelling) reflect the operational risk profile and are of good quality.

In other words any under- or over-evaluation of frequency or severity needs to be corrected in the data quality assurance process. Techniques used in validation include the "two pairs of eyes principle", internal audit of the risk assessment process, comparison of actual losses against experts' expectations, comparison of the outcome of scenario assessments against internal audit findings, and challenge by Group functions such as Risk.

### 1.2.4 Determination of Parameter Values

In the fourth step any required parameter values to be employed in the model for distributions or analytical solutions are determined from the scenario assessment data, once they have been quality assured.

For instance, if the model employs an individual frequency and severity distribution for each cell of the matrix that combines scenario classes and organisational parts, each frequency and severity distribution must be provided with its individual parameter values, i.e. usually at least mean and standard deviation. The parameter values for each individual distribution can be determined by utilising the usual statistical techniques on the data that results from the scenario assessments, which fall into the same cell. This is illustrated in figure 4 below.



| | Raw Data AFTER data cleansing | | | | *Parameter Estimates for Distribution* | | | |
|---|---|---|---|---|---|---|---|---|
| **Scenario Class** | **Typical Frequency** | **Frequency Upper Bound** | **Typical Severity** | **Severity Upper Bound** | ***Mean Frequency*** | ***Standard Deviation*** | ***Mean Severity*** | ***Standard Deviation*** |
| **IT** | | | | | ***4*** | ***2*** | ***200*** | ***233*** |
| * Scenario 1 | 1 | 6 | 50 | 300 | | | | |
| * Scenario 2 | 6 | 10 | 300 | 1000 | | | | |
| * Scenario 3 | 5 | 7 | 250 | 700 | | | | |
| **Control** | | | | | ***6*** | ***3*** | ***250*** | ***125*** |
| * Scenario 1 | 3 | 6 | 100 | 500 | | | | |
| * Scenario 2 | 7 | 10 | 400 | 100 | | | | |
| * Scenario 3 | 8 | 20 | 250 | 900 | | | | |
| ... | | | | | ... | ... | ... | ... |

*Figure 4: Scenario assessment and determination of parameters*

### 1.2.5 Model and Parameters

The fifth step deals with the application of the model, which means that at this point in time the model must already exist. This is important because the risk model also reflects the scenario classes and determines the necessary parameter values. How to build a good risk model has been described in more detail above.

In this step the determined parameters are fed into the risk model. The usual models use Monte-Carlo-simulation techniques to compound all individual distributions per scenario class and organisational unit into an overall aggregated potential loss distribution. As an alternative analytical models may be used.

Basically, a Monte-Carlo simulation is a big dice-rolling exercise where the dice are shaped such that their different sides fall with different frequencies (given by the corresponding distributions). One set of dice is for the frequency distributions, the other set for the severity distributions. Each iteration starts with a roll of one of the frequency dice. The number that falls determines how often the corresponding severity die has to be rolled. Say, for instance, the frequency die shows 3. This means that we roll the corresponding severity die 3 times. The severities are all added up to make the potential loss for this iteration. This procedure is repeated many times, resulting in the corresponding number of potential losses. The histogram of these potential losses makes up the overall aggregated loss distribution. The overall procedure and the resulting aggregated potential loss distribution are illustrated in figure 5.

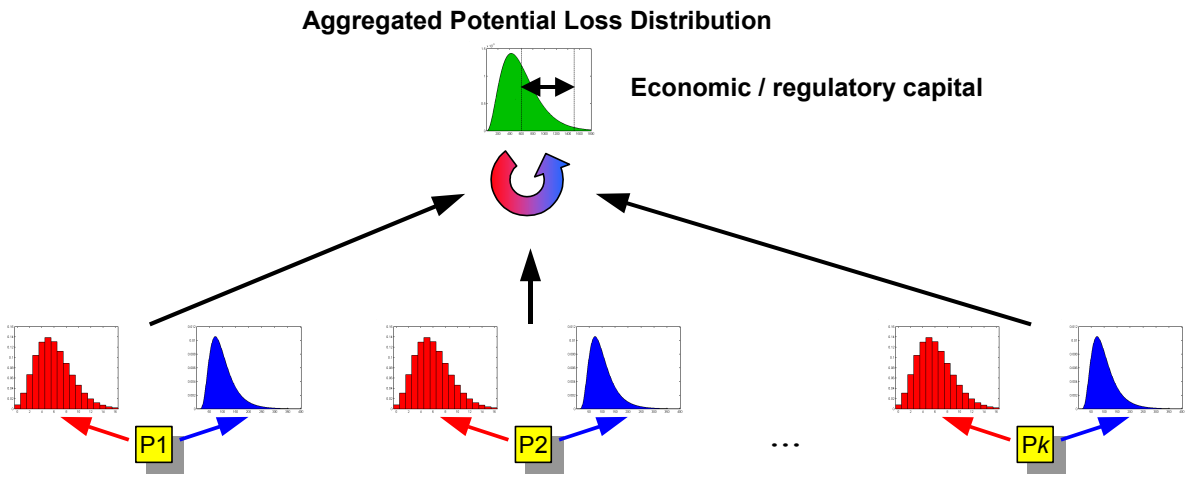



*Figure 5: Compounding distributions with parameter values P1…Pk by help of Monte-Carlo*

### 1.2.6 Model Output

The sixth step of the sbAMA is the output of the risk capital model. From the overall loss distribution values for economic or regulatory capital can be derived by identifying the quantile we are interested in. The quantile is the absolute value that corresponds to a given percentile. For example,the 99-percentile of the histogram of these potential losses is reflected by the amount that is greater than 99% and smaller than 1% of all potential losses. The difference between the quantile corresponding to the percentile in the tail (say 99%) and the mean of the distribution is the *economic capital* for the chosen percentile. The mean is sometimes called *expected (potential) loss* and the difference between the quantile and the expected loss is usually called *unexpected (potential) loss.*

Further, valuable management information can be derived from the calculations. It can easily be demonstrated how much a different scenario assessment affects the overall model outputs in terms of economic or regulatory capital. This not only provides a basis for sensitivity analysis on the model but also produces the right incentive since managers can, ex ante, see the effect on risk capital that can be achieved by improving their operational risk profile.

# 2 Discussion of a sbAMA

## 2.1 Comparison of sbAMA with other AMAs

The previous sections describe the core components, the overall process and main features of a sbAMA. This approach is closely aligned to how the business is managed. Its starting point is a consideration of the key risks to current and planned activities, in order to identify potential loss severities and their likelihood. All relevant management information is used in this assessment.

There are some similarities with other approaches. For instance, both the loss distribution and scenario-based approaches employ a statistical model that is founded on the amalgamation of frequency and severity distributions by methods such as Monte Carlo Simulation. The two approaches recognise that historical loss data alone are not sufficiently forward looking, and hence the LDA relies on scenarios where data are sparse.

At the same time a scenario-based approach has similarities with a scorecard approach, as both are sensitive to changes in the actual operational risk profile in an organisational part. Furthermore, the two approaches utilise expert opinion in the assessment of operational risk.

In the ways illustrated above a scenario-based approach can be said to bridge the gap between the loss distribution and scorecard approaches.

## 2.2 Benefits of sbAMA

A sbAMA is inherently forward looking and is therefore able to respond at an early stage to any changes. This responsiveness is well suited to a dynamic business and organisational environment and supports a proactive risk management culture. As well as making full use of expert opinion a sbAMA also takes into account empirical data such as internal losses, relevant external losses or key risk indicators.

The process of generating and assessing scenarios as well as evaluating the quality of the associated risk factors and control environment provides an important flow of management information. This can be used as the basis for risk management decisions, for example to establish the priorities for reducing risk by improving the quality of specific risk factors or controls. Any such change in the organisation's risk profile should prompt a re-assessment of the corresponding scenarios. For example, if an increase in risk is introduced through the purchase of a new business, then this will be reflected in increased frequency and/or severity estimates and a higher capital requirement. Correspondingly, a reduction in frequency and/or severity estimates, for example through improved controls, will generate a lower capital requirement. By creating an incentive framework in this way a sbAMA facilitates a progressive process of improvement in operational risk management.

The close involvement of risk takers in all organisational parts increases the transparency of the process and raises risk awareness. The process is clearly seen to be business specific and has the flexibility to adjust to the particular needs of an organisational part. Being embedded in this way contributes to meeting the Basel 2 use test requirement.

# 3 Conclusion

At the heart of a sbAMA and underpinning its conceptual soundness is the use of "what-if" questions to give a forward looking direction to the risk assessment process. The scenario-based approach shares a number of features in common with other conceptual AMAs such as the use of expert opinion and a statistical model.

A sbAMA integrates all significant elements required for comprehensive risk assessment. By blending empirical data with expert opinion an organisation is able to learn from its past experience and take account of the changes inherent in a dynamic business environment. Involving risk takers in the assessment process and using the results to create incentives for better risk management meets the AMA "use test" requirement.

# 4 Glossary, Definitions and Illustrations

**Risk:** Risk is the combination of severity and frequency of potential loss over a given time horizon. Risk can be expressed in the dimensions of **potential loss severity** and **potential loss frequency** with the measuring units of [monetary unit; no. of times per year], e.g., potentially €10,000 potentially 3 times in 1 year, or potentially €15,000 potentially 4 times in 1 year, or potentially €500,000 potentially 1 time in 100 years. The risk is higher if it is greater in at least one dimension and at least the same in the other. Risk is a reflection of vulnerability. The evaluation of risk should focus on vulnerabilities. Risk can be reduced by transferring it or by improving the quality of underlying risk factors.

**Quality:** Quality is defined as "the totality of features and characteristics […] that bear on its ability to satisfy stated or implied needs." (ISO 9000:2000). According to this definition, useful dimensions to evaluate the quality of risk factors could be suitability & functionality, security & reliability, and availability & accessibility. Quality is usually measured in scales such as *good, medium, poor,* scores such as *3 out of 10,* percentages such as *50%,* traffic light colours such as *green, amber, red*.

**Risk Factors:** A risk factor is a factor to which an operational entity is vulnerable if it fails, deteriorates or is of poor quality. Risk factors are the critical resources on which businesses depend and are sometimes also called operational risk drivers. Common operational risk factors are: *Human expertise / knowledge, Management, Internal services / Information, External services / suppliers, Information technology, Infrastructure (Office communication, LAN, premises, etc.), Controls against unauthorised activities or unintentional errors, Controls against external criminal activities, Preparation for external events (e.g. catastrophes), Legal requirements.*

**Scenario:** A scenario is something tangible that could happen in the future (i.e. a potential event) whilst an event is something concrete that has happened in the past. Events can have one or more causes and one or more effects (impacts). A generic scenario is a scenario that is derived from a generic class of scenarios (such as break-down of critical IT) by applying it to a defined area (such as FX-settlement). A stress scenario is a scenario of assumed potential high severity that is taken from a class of potential events, which happen very rarely (such as Barings). An appropriate scenario is a scenario that is appropriate for evaluating a certain risk type (such as market risk, credit risk, operational risk). A set of representative scenarios is a set that essentially represents all the risk factors for the risk type in question.

**Risk Capital:** Risk Capital is the amount of capital to protect the company with a certain probability against insolvency due to high severity losses. Risk Capital therefore expresses the overall potential loss severity for a given potential loss probability. Risk Capital is the output from a risk model. Risk Capital must be justifiable in size and based on consistent modelling across and within organisations. Regulatory Capital is Risk Capital for which the regulators set the probability. Economic Capital is Risk Capital for which the probability is determined by help of internal economic reasoning, i.e. an internal model. The computation of Economic Capital and Regulatory Capital should ideally result from the same model. However, the model parameters and assumptions may differ due to a differing rationale or restriction set by the regulators.