Scenario-based AMA

Presentation for RMG-Conference 29./30. May 2003
May 2003 (final version 1.0)

The following banks have contributed to the content and drafting of the presentation. 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.

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
Outline of presentation

- Objectives of presentation
- Introduction
- Overview of concept
- How to determine appropriate scenarios for OR?
- How to ensure that scenarios are consistent, relevant and capture all material OR?
- How to evaluate scenarios in an organisation?
- How to use scenarios for modelling purposes?
- Why a scenario based AMA improves OR management (example application)
- Key benefits of a scenario based AMA
- How other building blocks link into a scenario based AMA
- Overlap / similarities with LDA / Scorecard
- Illustrations
Objectives of the presentation

- To demonstrate that a scenario based approach is conceptually sound
- To define the key features of implemented scenario-based AMA approaches
- To prove that a scenario based approach is a valuable basis for managing risks
- To indicate that banks are fairly aligned in terms of thinking about scenarios
- To describe how scenarios can form an integral part of economic and regulatory capital calculations
- To illustrate how scenarios can be constructed in the most useful way
Executive Summary

A scenario based AMA

- is focused on a forward looking assessment of the key operational risks in an organisation taking into account both the internal control environment and external threats
- is an approach that employs the technique of individual scenario evaluation in a similar fashion to market and credit risk
- is based on all available information (expert experience, internal / external losses, KRIs, quality of control environment)
- leads via a model to a sound economic capital number that helps to incentivise prudent and pro-active OR management
- bridges the gap between LDA and Scorecard approach (or at least has a considerable overlap with each)
- has been or is being successfully implemented in a number of international banks
Introduction

- Scenarios are defined as potential events (i.e. events that could happen in the future).

- Risk is inextricably linked to the evaluation of "what-if" certain scenarios occur. The evaluation process involves providing answers to two fundamental questions:
  - How likely are certain scenarios to happen?
  - How severe could their impact be?

- Scenarios are already an important technique in the evaluation of market and credit risk as illustrated in the following questions:
  - *What is the impact if the yield curve shifts by 20bp? How likely is this?*
  - *What is the impact if this customer defaults? How likely is this?*

- Scenarios are also an essential component in the assessment of operational risks and determination of capital.
Overview of concept

<table>
<thead>
<tr>
<th>Scenario Generation</th>
<th>Scenario Assessment</th>
<th>Data Quality</th>
<th>Determination of Parameter Values</th>
<th>Model &amp; Parameters</th>
<th>Model Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to determine appropriate scenarios for OR?</td>
<td>How to evaluate scenarios in an organisation?</td>
<td>How to use scenarios for modelling purposes?</td>
<td>Mean, Std. deviation, etc.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

How to ensure that scenarios are consistent, relevant and capture all material OR?

<table>
<thead>
<tr>
<th>Scenario Classes</th>
<th>Organisational Parts</th>
</tr>
</thead>
</table>

Data Quality:
- 275.26
- 127.69
- 574.68
- 892.72
- 449.62
- 688.35
- 694.28
How to determine appropriate scenarios?

- The determination of appropriate scenarios that are representative for OR is key to the scenario based AMA.

- **Scenario classes** – one or more – are classes that are derived from loss event types or risk factors and that contain scenarios. (Example: Scenario class = IT-break down.)

- **Organisational parts** are the parts of the organisation for which OR is separately evaluated.

- Generate scenario(s) per scenario class and organisational part based on:
  - guided discussions with the business in workshops (eg. Dresdner; Fortis, HBOS)
  - a matrix of „critical resources and states of risk“ (eg. Banca Intesa)
  - weaknesses per risk factor (eg. UFJ Holdings)
  - a specification of critical resources and failure periods by the organisational parts (eg. Dresdner)
  - addressing particular management concerns (all)

- All scenarios are fully documented to allow independent review and assessment.
How to ensure that scenarios are consistent, relevant and capture all material operational risks?

- **Consistent?**
  - Every organisational part must consider as a minimum each of the common set of scenario classes, thereby achieving consistency of the overall framework.
  - Techniques such as workshops assist to achieve consistency of scenarios across organisational units.
  - Review by Internal Audit and Risk Functions provides further consistency between organisational parts.

- **Relevant?**
  - Every organisational part assesses the relevance of all scenarios to its business thereby ensuring relevance to them (e.g. if a org-unit is not dependent on IT, it does not make sense to evaluate the risk due to IT break-down).

- **Capture all material operational risks?**
  - The techniques to determine the scenario classes (eg use of expert judgement and historical loss data) maximise coverage of known and foreseen risks.
  - This coverage is further enhanced when applied to the organisational parts and discussed with them to ensure that their specific risks are covered.
How to evaluate scenarios in an organisation?

- For each scenario banks assess potential loss frequencies and potential loss severities.
- The organisational process of evaluation is based on:
  - questionnaires
  - guided workshops
  - central (management) expertise
- In order to come up with plausible answers banks base their evaluation on information relevant to the scenario, such as
  - an assessment of operational quality / quality of control environment
  - past losses, key risk indicators, insurance
  - industry and managerial experience
- To validate the scenario evaluations banks apply techniques such as
  - 4-eye principle
  - Internal audits of assessment process and resulting quality
  - Comparison between actual losses and expert expectations
  - Consistency checks (e.g. psychometric analysis, Group functions challenge profiles of organisational parts, comparison to internal audit findings and validation.)
How to use evaluated scenarios for modelling purposes?

- A good risk model must be **consistent, robust, and stable over time**, so that changes in economic capital result from changes in the underlying risk profile and not from changes in the model.
- A model on risk requires **plausible assumptions** where distributions or analytical solutions are used.
- The model requires the **estimation of its parameters**.
- The data required for the parameter estimation must go through a rigorous data **quality assurance**.

<table>
<thead>
<tr>
<th>Scenario Class</th>
<th>Typical Frequency</th>
<th>Frequency Upper Bound</th>
<th>Typical Severity</th>
<th>Severity Upper Bound</th>
<th>IT</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>* Scenario 1</td>
<td>1</td>
<td>6</td>
<td>50</td>
<td>300</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>* Scenario 2</td>
<td>6</td>
<td>10</td>
<td>300</td>
<td>1000</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>* Scenario 3</td>
<td>5</td>
<td>7</td>
<td>250</td>
<td>700</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Scenario 1</td>
<td>3</td>
<td>6</td>
<td>100</td>
<td>500</td>
<td>6</td>
<td>250</td>
</tr>
<tr>
<td>* Scenario 2</td>
<td>7</td>
<td>10</td>
<td>400</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Scenario 3</td>
<td>8</td>
<td>20</td>
<td>250</td>
<td>900</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Raw Data AFTER data cleansing**

**Parameter Estimates for Distribution**

<table>
<thead>
<tr>
<th>Mean Frequency</th>
<th>Standard Deviation</th>
<th>Mean Severity</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>233</td>
<td>250</td>
<td>125</td>
</tr>
</tbody>
</table>
Why a scenario based AMA improves OR management

- In order to reduce risk OR managers may decide to improve the quality of their risk factors (such as controls, IT, special knowledge, etc.)
- The process of evaluating and analysing the risk factors and controls associated with scenarios provides important information on how to improve OR management.
- Once such improvements have been achieved, i.e., organisational parts have reduced their operational risk profile, the corresponding scenarios can be reassessed.
- If the re-assessment leads to lower frequency and severity estimates this will result in a lower economic capital requirement.
- In this way an incentive is created to improve the quality of their risk factors.
- This in turn leads to an improvement in overall OR management.
Key benefits of a scenario based AMA

- Forward looking, pro-active risk management
- Direct link to the management process (use test)
- Takes account of internal losses, KRI and external events
- Responsive to changes in the environment
- Immediately incorporates changes in the organisational environment
- Focuses on „key risk exposures“ material exposures
- Relatively transparent
- Supports risk culture
- Incentivises risk management
- Strong link between controls and risk
- Linkage between economic / regulatory capital and business risk profile
- Business specific / flexible to adjust to the business needs
- Helps identify mitigation priorities (cost/benefit)
How other building blocks (Losses, KRIs, Control Environment) link into scenario based AMA

**Scenario Generation:**
- External losses to build sensible scenarios
- Loss types to devise sensible scenario classes

**Scenario Evaluation:**
- Loss data where available as a mean to assess scenarios or to validate expert evaluations
- External loss data where available to help assess certain scenarios
- Key risk indicators to validate the assessment of certain scenarios
- Quality of control environment is considered when assessing frequency and severity of the scenarios and in some cases explicitly rated.

**Model building:**
- Historical losses where available to determine and justify assumptions about statistical distributions in the risk capital model

**Validation of aggregated potential loss distribution:**
- Historical losses to check on plausibility of certain quantiles of aggregated potential loss distribution
Example of how other building blocks link into scenario assessment

- External loss data, loss event types and knowledge about necessary operational resources generate the following scenario:

- What if a particular IT-system (e.g. a key payments system) breaks down for a critical time period?

- An expert in payments systems estimates on the basis of his experience:
  - a potential loss severity for this scenario of $100,000
  - a potential loss frequency for this scenario of 1 in 5 years.

- An analysis of past losses shows that he has indeed estimated a reasonable severity number.

- An analysis of the corresponding key risk indicators (e.g. system downtime / IT staff turnover) shows, however, that he has underestimated the potential loss frequency which will subsequently be corrected in the data quality assurance process.

- Thus other building blocks can be used both to generate scenarios and assure the quality of the assessment thereby influencing the resulting economic capital.
Overlap / similarities with LDA and Scorecard Approach

An „Scorecard Approach“ and a Scenario based AMA both

- employ scenarios to be evaluated as part of the „scorecard“
- are sensitive to changes in the actual operational risk profile in an organisational part
- make use of expert opinion as part of the data to assess the operational risk

A Loss Distribution Approach and a Scenario based AMA both:

- employ a statistical model
- recognize the fact that loss data alone is not forward looking
- rely on scenarios where losses are sparse
Illustrations

Overview of implemented industry practices
How to determine appropriate scenarios?
<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Risk Factor</th>
<th>n°</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employer Risk</td>
<td>Strikes</td>
<td>1</td>
<td>due to fraud/theft by employees?</td>
</tr>
<tr>
<td>Employer Risk</td>
<td>employee compensation</td>
<td>2</td>
<td>due to unauthorised activities by employees</td>
</tr>
<tr>
<td>Employer Risk</td>
<td>Discrimination</td>
<td>3</td>
<td>arising from the misuse of privileged information by employees?</td>
</tr>
<tr>
<td>Employer Risk</td>
<td>Theft/fraud unauthorized activity</td>
<td>4</td>
<td>due to worker disputes or organized labour activity (strikes)?</td>
</tr>
<tr>
<td>Employer Risk</td>
<td>Confidentiality</td>
<td>5</td>
<td>arising from employer liability (employee compensation and benefit)?</td>
</tr>
<tr>
<td>Employer Risk</td>
<td>Workplace safety</td>
<td>6</td>
<td>due to workplace security issues or non compliance (employee/third party)?</td>
</tr>
<tr>
<td>Employer Risk</td>
<td>Uncovered</td>
<td>7</td>
<td>due to lack of compliance/non observance or external regulation?</td>
</tr>
</tbody>
</table>
We have defined 10 risk factors, that we believe are the most important usual resources in any process or any organisational part in any organisation.

For these 10 risk factors we have build 10 scenario classes, i.e. the resource fails, breaks down, is of poor quality, does not work, is not existent etc.

**Example:**

*Resource* = IT.

*Generic scenario class* = IT breaks down critical time period.

*Organisational part* = Front office equity trading.

*Specified scenario* = IT-system (e.g. Imagine) for equity trading breaks down 1 day.

In order to determine specific scenarios that are meaningful for a particular organisational part, we ask whether each scenario class is relevant for the organisational part in question. If yes, scenarios of this class are specified and evaluated by experts of the organisational part.
We have defined a comprehensive list of risk factors (resources). The criticality of each risk factor is analysed together with the business during the yearly self-assessment exercise.

One scenario is built for each identified critical resource. The scenario consists of the non-availability of one specific critical resource. It involves frequency and severity estimations relative to the current situation.
Every organisation unit in the Group (currently approx. 370) completes a semi annual self-assessment (scenario) profile.

The risks and risk scenarios are based on a 3 tiered categorisation framework, tier 1 being people process, systems, external and business (shown above).

The process involves considering internal & external losses, together with changes in the businesses environment relating to the categorisation framework.

It is a Group-wide exercise with the ability to cross reference risks and responsibility between business areas (i.e. Where the potential impact will effect one area but the process is owned in another).
- Self risk assessment are made via group-wide tools for every material process/system.
- Weaknesses against operational risk events are identified for each process/system via standard assessment keys.
- The risk assessment process involves evaluating the control level and considering changes in the business environment.
- Completed evaluation sheets are scored by using a scoring table which assigns a score to each assessment key.
- Higher-scored processes/systems are eligible for scenario generation.
How to evaluate scenarios in an organisation?
Banca Intesa

• The scenario forms (questionnaires) are distributed by an Intranet based (Java) assessment tool (GARI)

• Each questionnaire refers to a part of the organisation based on an organisational mapping. The Head of each Division or department executes the assessment

• The results of each questionnaire is validated by Internal Audit and the Security Office

<table>
<thead>
<tr>
<th>Inputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Internal/External Loss Data</td>
</tr>
<tr>
<td>- KRI / Last years SRA</td>
</tr>
<tr>
<td>- Audit &amp; security reports</td>
</tr>
<tr>
<td>- ORM correspondents</td>
</tr>
</tbody>
</table>

| Organizational structure of the bank |
| Risk Class Model |
| Predefined severity/WC classes |

© Scenario-based AMA working group
Risk scenarios are evaluated by relevant business expertise either through a facilitated risk workshop or through self assessment questionnaires.

Key inputs into the evaluation are Loss experience, KRIs and Audit Information.

The appropriateness and effectiveness of the controls are assessed and a decision taken whether further investment is required in controls or whether the risk is within appetite and should be accepted in line with Group Risk Acceptance Policy.
The scenarios are distributed by a Web-Tool called TESSA (a module of ORTOS)

The distribution follows a defined workflow.

Each questionnaire refers to a part of the organisation based on an organisational mapping.

For each organisational part an assessor and an approver are determined.

The assessors fill in the questionnaires, the approvers approve them.

Questionnaires also serve as a guidance for workshops.

Subsequently the analysis and quality assurance take place.
The scenarios are stored in a central database (OPERA) and are reviewed on yearly basis.

Scenarios are currently built for each organisational part, i.e. business line/legal entity. Scenario outcomes, together with self-assessment results, KRIs, loss experience, etc, are discussed with the business risk management team/business risk committee.
Halifax Bank of Scotland

- Delivered through AspectsOR, an inhouse built, intranet based tool.
- Facilitated workshops define the scenarios (full training undertaken, including lessons learnt, for the facilitators after each exercise).
- Identify 2 scenarios per risk, most likely and worse case scenario.
- A residual and average risk exposure figure is then calculated per risk within AspectsOR.

Business units complete Operational Risk Profiles (ORP) at all levels.

- Annual loss distribution obtained on the basis of the scenario results by convolution.
- Correlation between risk types introduced via monte carlo, preformed with a common seed.
- Potential double counting of risk is mitigated by aggregation and adopt functionality in AspectsOR.
Operational loss “generic scenarios” and “stress scenarios” are created for the weaker (or, “higher-scored”) processes/systems.

Scenario worksheets which are group-wide tools are distributed in Excel format.

The expert, who completed the original risk assessment, create the scenario.

Risk management sections verify the scenarios.
What do reports resulting from assessments look like? What are the dimensions on which reports are based?
Dimensions:
- Risk factor
- Description of scenario
- Potential loss frequency
- Potential loss severity (average + worst case)
- EL + CaR (Gross)
- Rating
- Vulnerability type
- Quality of control
- Mitigation Type
### General Info

<table>
<thead>
<tr>
<th>No</th>
<th>Type</th>
<th>Cluster</th>
<th>SBU</th>
<th>Business Activity</th>
<th>Risk Description</th>
<th>Con Effect</th>
<th>Freq</th>
<th>Impact (£m)</th>
<th>Fin Loss (£m)</th>
<th>Fin Loss Rep Dam</th>
<th>Staff Diss/Welfare Erosion</th>
<th>Service Failure</th>
<th>Reg/Legal non Comp</th>
<th>Mit %</th>
<th>Overall Risk Rank</th>
</tr>
</thead>
</table>

- The outputs of the scenario assessments feed the Business Area and Group Risk Profile Reports.
- The output informs management action including investment in controls, risk transfer and capital allocation.
- The scenario ‘potential loss’ data is modelled in conjunction with actual internal loss data to calculate the economic capital requirement for Business Areas and the Group.

### Outputs include:

- Risk description
- Frequency
- Impact
- Annualised Financial Loss
- Indirect Impacts
- Level of Mitigation
- Required Management Actions
Dimensions:
- Organisational part
- Risk factor
- Nb relevant scenarios
- Potential loss frequency
- Potential loss severity
- Standard risk cost
- Quality of risk factor
A group-wide operational risk report is built each quarter.

Scenarios are used for the calculation of sensitivity ($\Delta$VaR) to non-availability of a risk resource.

Although scenarios are used in the operational risk management process, they do not contribute directly to the calculation of economic capital, which is performed on the basis of loss data with defined qualitative adjustment.
Halifax Bank of Scotland

- Tailorable summary views in AspectsOR for users (dummy example shown below).
- Automated paper based reporting generated around risk categories, business units, action plans etc.

A Group-wide operational risk report is produced semi annually for the Board and Audit Committee. Results from the scenario exercise are used with other OR information including losses, project risk data etc.

Comparisons drawn against other operating measures (dummy example shown above)
# Risk Assessment Report (System Risk)

## Result of System Risk Evaluation

<table>
<thead>
<tr>
<th>Level of Importance</th>
<th>March 2002</th>
<th>Mar 2001</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Risk Level</td>
<td>System</td>
</tr>
<tr>
<td>A</td>
<td>Low</td>
<td>XX</td>
</tr>
<tr>
<td></td>
<td>Acceptable</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>XX</td>
</tr>
<tr>
<td>B</td>
<td>Low</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Acceptable</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>XX</td>
</tr>
</tbody>
</table>

### SYSTEM

<table>
<thead>
<tr>
<th>SYSTEM</th>
<th>SCENARIO</th>
<th>Standard</th>
<th>Frequency</th>
<th>Severity</th>
<th>Fre .</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Computer Center Breakdown by Earthquake</td>
<td></td>
<td>XX</td>
<td>XXXX</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>&quot;Online&quot; Breakdown by Earthquake in Tokyo pref.</td>
<td></td>
<td>XX</td>
<td>XXXX</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Earthquake in Osaka prefecture</td>
<td></td>
<td>XX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>&quot;Online&quot; Breakdown in Osaka pref.</td>
<td></td>
<td>XX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Main Accounting System Breakdown</td>
<td></td>
<td>XX</td>
<td>XXXX</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>&quot;Online&quot; Breakdown in Nagoya pref.</td>
<td></td>
<td>XX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>&quot;Banking Association Network&quot; breakdown</td>
<td></td>
<td>XX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>ATM theft</td>
<td></td>
<td>XX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Fraud (using forged Bankcard)</td>
<td></td>
<td>XX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Miss Operation in Computer Center</td>
<td></td>
<td>XX</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Dimentions
- System/Process
- Type of loss event
- Risk Factor
- Description of scenario
- Potential loss frequency
  - Standard risk cost
  - Stress case
- Potential loss severity
  - Same as above
- Operation volume
What distributional assumptions are you making in your risk capital model?
Choice of distributions and qq-plots

Severity distributions:
- **Lognormal**: Credit Lyonnais, Dresdner Bank, HBOS
- **Normal Gamma**: Fortis, Dresdner Bank
- **Others, e.g. Gumbel, Weibull, Frechet**: Banca Intesa, Halifax Bank of Scotland

Frequency distributions:
- **(Negative) Binomial distribution**: Dresdner Bank, Fortis
- **Poisson**: Banca Intesa, Credit Lyonnais, Dresdner Bank, UFJ Holdings

Dresdner Bank: qq-plot for OR losses

HBOS: qq-plot for OR losses > £10,000