Operational Risk Scenario Analysis

17/03/2010
Michał Sapiński
michal.sapinski@statconsulting.com.pl
Operational Risk - ‘Tail Events’
Agenda

Operational Risk - Scenario Analysis

- Operational Risk - Definition
- Solvency II
- Role of Scenarios in Risk Management
- Role of Scenarios in Risk Quantification (VaR)
- Summary
Operational Risk

- Operational risk means the risk of loss arising from inadequate or failed *internal processes, personnel* or *systems*, or from *external events*.

- Operational risk shall *include legal risks* and *exclude* risks arising from *strategic decisions*, as well as *reputation risks*.

- The capital requirement for operational risk shall reflect operational risks to the extent they are not already reflected in the risk modules.

SOLVENCY II DIRECTIVE, 25 November 2009
Operational Risk
Solvency II/Basel II

Solvency II

Operational risk is the risk of loss arising from inadequate or failed internal processes, people, systems or external events.

Operational risk also includes legal risks.

Reputation risks and risks arising from strategic decisions do not count as operational risks.

Basel II

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 reputation risk.
Operational Risk Types

- **Internal Fraud** - Unauthorized activity, theft and fraud
- **External Fraud** - theft of information, hacking damage, third-party theft and forgery
- **Employment Practices and Workplace Safety** - discrimination, workers compensation, employee health and safety
- **Clients, Products, & Business Practice** - market manipulation, antitrust, improper trade, product defects, fiduciary breaches, account churning
- **Damage to Physical Assets** - natural disasters, terrorism, vandalism
- **Business Disruption & Systems Failures** - utility disruptions, software failures, hardware failures
- **Execution, Delivery, & Process Management** - data entry errors, accounting errors, failed mandatory reporting, negligent loss of client assets
Operational Scenarios, Events, Losses

- **Scenario** - Class of Operational Events

- **Event** - An *operational risk event* is an incident leading to the actual outcome(s) of a business process to differ from the expected outcome(s), due to inadequate or failed processes, people and systems, or due to external facts or circumstances (ORX).

- **Loss** - An *operational risk loss* is a negative impact on the earnings or equity value of the firm due to an operational risk event (ORX).
Operational Risk

Risk of loss arising from inadequate or failed internal processes, personnel or systems, or from external events

Risks
Processes, People, Systems, External Events

Events

Losses
{ Frequency, Severity }
Solvency II - Three Pillars

**Pillar I**
- Technical Provisions
- **MCR** (Minimal Capital Requirement)
- **SCR** (Solvency Capital Requirement)

**Pillar II**
- Corporate Governance
- **ORSA** (Own Risk and Solvency Assessment)
- Principles for internal control and risk management

**Pillar III**
- Reporting
- Market Discipline
SCR (Solvency Capital Requirement): Standard Formula

QIS4 - Technical Specifications
QIS4 - Operational Risk
Standard Method SCR

\[ SCR_{op} = \min \left\{ 0.30 \cdot BSCR; \, Op_{ln \cdot ul} \right\} + 0.25 \cdot Exp_{ul} \]

\[ Op_{nl \cdot ul} = \max \left\{ \begin{array}{l}
0.03 \cdot (Earn_{life} - Earn_{life \cdot ul}) + 0.02 \cdot Earn_{nl} + 0.02 \cdot Earn_{h} ; \\
0.003 \cdot (TP_{life} - TP_{life \cdot ul}) + 0.02 \cdot TP_{nl} + 0.002 \cdot TP_{h}
\end{array} \right\} \]

\[ \begin{array}{ll}
TP_{life} &= \text{Total life insurance technical provisions (gross of reinsurance)} \\
TP_{life \cdot ul} &= \text{Total life insurance technical provisions for unit-linked business (gross of reinsurance)} \\
TP_{nl} &= \text{Total non-life insurance technical provisions (gross of reinsurance)} \\
TP_{h} &= \text{Total health insurance technical provisions (gross of reinsurance)} \\
Earn_{life} &= \text{Total earned life premium (gross of reinsurance)} \\
Earn_{life \cdot ul} &= \text{Total earned life premium for unit-linked business (gross of reinsurance)} \\
Earn_{nl} &= \text{Total earned non-life premium (gross of reinsurance)} \\
Earn_{h} &= \text{Total earned health insurance premium (gross of reinsurance)} \\
Exp_{ul} &= \text{Amount of annual expenses (gross of reinsurance) incurred in respect of unit-linked business} \\
BSCR &= \text{The basic SCR}
\end{array} \]

Źródło: QIS4
Operational Risk Management

Loss Database

KRI

Scenario Analysis

History

Now

Future

Precise qualitative and quantitative operational risk assessment
Operational Risk Management

KRI

Scenario definition - based on occurring losses or loss possibility

Losses

Analysis KRI selection

KRI identification and definition

Scenarios

Risk types

Business Lines

Processes

Units

Products

Systems
Scenario Analysis

- Once an year, owners of the processes are collecting operational scenarios
- Every scenario describes the possibility of occurrence of operational loss.
- Scenarios besides description have the following properties
  - Risk type, line of business, process, business unit
  - Risk control level, possible enhancements in risk control level
  - Business continuity plans
- Quantitative information
  - Frequency
  - Severity
Scenarios - Sources of Information

- Internal Loss Data
- External Loss Data
- Imaginative Thinking

Scenario 1
Scenario 2
Homogeneous organization parts

Risks

Scenario: Server crash
- Frequency: 1-2 times per 5 years.
- Expected loss: 5-10k
- Unexpected loss: 50-60k

Insurance Company

Homogeneous
Independent
Clear

Business Lines x Processes

Risk Types
### Scenario Analysis - Scenario Example

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line of business:</td>
<td>Ubezpieczenia majątkowe</td>
</tr>
<tr>
<td>Process:</td>
<td>Zarządzanie sprzedażą online</td>
</tr>
<tr>
<td>Business unit:</td>
<td></td>
</tr>
<tr>
<td>Risk type:</td>
<td>Oszustwa zewnętrzne</td>
</tr>
<tr>
<td>Product:</td>
<td>-</td>
</tr>
<tr>
<td>System:</td>
<td>E-Sales</td>
</tr>
<tr>
<td>Scenario:</td>
<td>Włamanie do systemu i kradzież danych</td>
</tr>
<tr>
<td>Risk control level:</td>
<td>Nieakceptowalny</td>
</tr>
<tr>
<td>Enhancements in risk control:</td>
<td>Wprowadzenie dodatkowych zabezpieczeń i procedur</td>
</tr>
<tr>
<td>Connected KRI:</td>
<td>Rotacja pracowników w dziale IT, ...</td>
</tr>
</tbody>
</table>

**Quantitative information:**

- Occurrence frequency: 1-2 / 5 lat
- Severity (median): 30 000 - 40 000
- Stress severity: 100 000 - 300 000
- (Maximum severity):       
- Events/Losses list: ...
Scenario Analysis - VaR modeling

- Frequency, Severity distributions
- Comparison with collected loss data
- Aggregation, diversification
- **Result**: Aggregated operational risk loss distribution with decomposition

---

**Severity**

- Log-normal
- Gumbel
- Weibull

**Frequency**

- Negative binomial
- Poisson

---

Copyright by StatConsulting Sp. z o.o. 2010
Value at Risk

Expected Loss

Unexpected Loss

Extra capital for unexpected loss

Solvency II - 99.5

VaR 95% = 42 milionów EUR

Copyright by StatConsulting Sp. z o.o. 2010
### Scenario Analysis - VaR aggregation

#### Line of business

- **Whole company**

#### VaR process

**Scenario:** Whole company

<table>
<thead>
<tr>
<th>Event</th>
<th>VaR 95%</th>
<th>Value at Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>event 1</td>
<td>1209</td>
<td>1209.01</td>
</tr>
<tr>
<td>event 2</td>
<td>2354</td>
<td>2354.02</td>
</tr>
<tr>
<td>event 3</td>
<td>1234</td>
<td>1234.03</td>
</tr>
</tbody>
</table>

**Scenario:** Company X

<table>
<thead>
<tr>
<th>Event</th>
<th>VaR 95%</th>
<th>Value at Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>event 1</td>
<td>1209</td>
<td>1209.01</td>
</tr>
<tr>
<td>event 2</td>
<td>2354</td>
<td>2354.02</td>
</tr>
<tr>
<td>event 3</td>
<td>1234</td>
<td>1234.03</td>
</tr>
</tbody>
</table>

**Scenario:** Company Y

<table>
<thead>
<tr>
<th>Event</th>
<th>VaR 95%</th>
<th>Value at Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>event 1</td>
<td>1209</td>
<td>1209.01</td>
</tr>
<tr>
<td>event 2</td>
<td>2354</td>
<td>2354.02</td>
</tr>
<tr>
<td>event 3</td>
<td>1234</td>
<td>1234.03</td>
</tr>
</tbody>
</table>

**Scenario:** Company Z

<table>
<thead>
<tr>
<th>Event</th>
<th>VaR 95%</th>
<th>Value at Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>event 1</td>
<td>1209</td>
<td>1209.01</td>
</tr>
<tr>
<td>event 2</td>
<td>2354</td>
<td>2354.02</td>
</tr>
<tr>
<td>event 3</td>
<td>1234</td>
<td>1234.03</td>
</tr>
</tbody>
</table>
Scenario Analysis - Risk Maps

Loss frequency vs. Loss severity:

- **Recurring losses**: Low severity, high frequency.
- **Critical situation**: High severity, high frequency.
- **Essential risk (unexpected losses)**: High severity, low frequency.
- **Minor risk**: Low severity, low frequency.

**Actions**:
- **Fixing processes**
- **Critical situation management**
- **Continuation plans, insurance**
Operational Risk - Scenario Analysis Summary

Scenario Analysis

- **Advantages**
  - **Forward looking**
  - **Collected loss data** can be used as a valuable support
  - Allows you to implement **risk controls prior** to the loss occurrence
  - Allows **risk quantification** - VaR method
  - Allows **risk sources identification** (for example VaR drill-down)
  - Allows to present risk on **risk maps**

- **Disadvantages**
  - Labor-intensity - smaller in subsequent rounds - big proportion of the scenarios remains unchanged
Contact:

StatConsulting Sp. z o.o.
Wołodyjowskiego 38a,
02-724 Warsaw, Poland
phone: +48 22 847 97 17
fax: +48 22 499 45 31
e-mail: info@statconsulting.com.pl