Key Risk Indicators integrated into a single Operational Risk Management Reporting

Gez Llanaj - Risk Management Practice, SAS UK
Agenda

- Which Indicators are key?
  - Defining KRI’s
  - Implementing a KRI program: Benefits & Issues
- Key components and systems required to bring KRI’s to “life”
- Integration of KRI's into business performance data
- Making it happen - “SAS Integrated Operational Risk Reporting and Governance“
- Conclusion
KRIIs and BASLE II

Sound Practices for the Management and Supervision of operational Risk, 2003:

In addition to monitoring operational loss events, bank should identify appropriate indicators that provide early warning of an increased risk of future losses. Such indicators (often referred to as key risk indicators or early warning indicators) should be forward-looking and could reflect potential sources of operational risk such as rapid growth, the introduction of new products, employee turnover, transaction breaks, system downtime, and so on. When thresholds are directly linked to these indicators and effective monitoring process can help identify key material risks in a transparent manner and enable the bank to act upon these risks appropriately. (BASLE II)
KRI as “KEY” indicators

- Systemic
- Meaningful
- Objective
- Easy to collect
- Dynamic
- Frequency
- Organizational/Sectional
- Predictive/Current/Lagging
- Composite/individual
- Non – redundancy
- Comprehensiveness
- Audit-ability
Implementing a KRI program

- Vertical consolidation and reporting of data; information gathered from various silo systems
- Not all functions will lend themselves to KRIs in the same way;
- How to ensure changing circumstances do not alter risk priorities?
Implementing a KRI program

Challenges

- Correlation between KRIIs and events or losses;
- Linking KRIIs to loss events and self-assessment: integrated reporting;
- Embedding a proactive approach aligned with risk appetite and performance management
A Simple Truth…

...There is no substitute for the knowledge of 'expert opinions' within the business: KRIIs cannot be pulled out of a magic hat; qualified personnel from each function/business area will be able, through proper facilitation of the discussion, to find the right indicators for their area and for the risks they face...

...Creating the proper context...
Key components required to bring KRI’s to "life"

- An organisation needs an integrated operational risk system providing a common language and a framework which identifies areas of exposure and then allows…..
  - Metrics to be identified to measure, monitor and manage those exposures at different levels within the organisation
  - Data on losses, near misses and control failures to be recorded
  - Ongoing assessment of the exposure
  - Performance measurement around the exposure, including use of capital
SAS Industry Solutions
SAS Risk Intelligence
SAS Operational Risk Solution

Operational Risk

- Loss Data Collection/ RCSA/ KRI
- Self Assessment/SOX
- External Loss Data
- Analytics & Capital Calculation
- Integrated Reporting
- Risk Governance
- SAS Discovering OpRisk Management
KRI Data Collection

- SAS provides multiple ways of collecting KRI data
  - Web forms for KRI data collection – manual
  - Deploy SAS Data Access and Extraction tools to automatically collect KRI data periodically from pre-defined IT systems. E.g. staff turnover data for various business units can be automatically extracted from HR systems (Peoplesoft, SAP, Oracle others). SAS has capabilities to extract data from 100+ types of data sources like Oracle, Peoplesoft, SAP, DB2, Excel, Access, CSV etc.
  - Data from any current system for KRI collection can also be directly read in the SAS Risk Dashboard.
KRI Data Collection

Data Quality

- Data quality is always highlighted as the biggest issue in every operational risk project. This is especially true in the area of Key Risk Indicators as these come from multiple sources and have different interpretations and usage.

- SAS Risk Dashboard provides a powerful data cleaning and validation engine to ensure that only valid data is surfaced in the reports.
KRI reporting framework

You can start with spreadsheets, but in time should consider a professional solution

An IT system for KRI gathering and reporting is a sophisticated management information tool

**KRI Data Mgt & Reporting Spec**
- KRI measure/issue set up
- Product/process mapping
- Decentralised submission
- Multiple reporting streams
- Edit/report/read role-play
- Multi-dimension data capture
- Item or bulk upload capability
- Data drilldown/breakdown
- Comparatives/benchmarks
- Graphing/data visualisation
- Issue tracking & follow-up
- Action management & costing
- Scorecard report-writer
- Web report distribution

**Workflow Principles**
- Central control over corporate KRIs and Data Model
- Functional ownership of data reporting and editing
- All staff should be able to write an OR report for their user rights
- Multiple reporting streams

**Stage Name**
- KRI Setup & Maintain
- Assign & Raise Submissions
- Data Entry & Locking
- Produce Reports Review & Edit
- Distribution
Integration of KRI's into Operational Risk Management Reporting

Dashboard & Risk Performance Management

Diagnostics & Drill down

Analytics

Process View

Central Risk Intelligence Repository

Risk Intelligence Portal
Integrated Coherent view of Operational Risk Environment

Dashboard & Risk Performance Management

SAS Risk Intelligence Portal

Self-Assessment Data

Operational Risk KRIs

Global: Key Risk Indicators (Jan 2003)

- Number of Effective Controls
  - 111%
  - 470
  - 423
- Number of Ineffective Controls
  - 111%
  - 1.02
  - 0.92
- Total OpRisk Losses (£)
  - 1.07%
  - 9,951,000
  - 999,200
- Number of OpRisk Loss Events
  - 1.05%
  - 104
  - 99
- Number of Business units submitting loss data
  - 12.5%
  - 48
  - 38
- Total External OpRisk Losses (£)
  - 93%
  - 255,505,308
  - 274,696,213
- Number of External OpRisk Loss Events
  - 10.5%
  - 394
  - 382
- Number of Risk Assessment questionnaires in latest Self Assessment exercise
  - 112.8%
  - 161
  - 144
- Internal fraud related losses
  - 117%
  - 6,225,119
  - 5,335,560
- External fraud related losses
  - 99%
  - 15,294,787
  - 15,502,520
- Staff turnover (%)
  - 12.2%
  - 10.4
  - 8.5
- Number of Risk and Control related issues
  - 12.0%
  - 1.39
  - 1.10
- Number of Action Plans behind planned date
  - 68%
  - 1.3
  - 19
# KRI Alerts and Reporting

## SAS Risk Intelligence Portal

**Group and Business Line KRI**

**Global: Key Metrics, Score: 110.10 (Demo Bank Y5-Dec2004)**

<table>
<thead>
<tr>
<th>KRI Category</th>
<th>Status (%)</th>
<th>Current Period</th>
<th>Previous Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Effective Controls</td>
<td>111%</td>
<td>470</td>
<td>423</td>
</tr>
<tr>
<td>Number of Ineffective Controls</td>
<td>111%</td>
<td>102</td>
<td>92</td>
</tr>
<tr>
<td>Total OpRisk Losses (£)</td>
<td>107%</td>
<td>59,951,800</td>
<td>55,992,000</td>
</tr>
<tr>
<td>Number of OpRisk Loss Events</td>
<td>105%</td>
<td>104</td>
<td>99</td>
</tr>
<tr>
<td>Number of Business units submitting loss data</td>
<td>126%</td>
<td>43</td>
<td>38</td>
</tr>
<tr>
<td>Total External OpRisk Losses (£)</td>
<td>93%</td>
<td>255,505,308</td>
<td>274,666,213</td>
</tr>
<tr>
<td>Number of External OpRisk Loss Events</td>
<td>109%</td>
<td>394</td>
<td>352</td>
</tr>
<tr>
<td>Number of Risk Assessment questionnaires in latest self assessment exercise</td>
<td>112%</td>
<td>151</td>
<td>144</td>
</tr>
<tr>
<td>Internal fraud related losses</td>
<td>117%</td>
<td>5,225,119</td>
<td>5,335,580</td>
</tr>
<tr>
<td>External fraud related losses</td>
<td>99%</td>
<td>15,294,787</td>
<td>25,502,520</td>
</tr>
<tr>
<td>Staff turnover (%)</td>
<td>122%</td>
<td>10.4%</td>
<td>8.5%</td>
</tr>
</tbody>
</table>

**KRI Views**

- **Aggregated KRI**
  - Peter
- **KRI - Hardware Age**
  - This KRI is tracked for Hardware Failure risk event.
  - Peter
- **KRI - Number of users utilising the system**
  - This KRI is tracked for Hardware Failure risk event.
  - Peter
- **KRI - System stress testing results**
  - This KRI is tracked for Hardware Failure risk event.
  - Peter
- **KRI - Total utilised system capacity**
  - This KRI is tracked for Hardware Failure risk event.
  - Peter
- **Risk Mapping - Business Process Driven Approach**
  - Peter
Diagnostics and drill down functionality

```
<table>
<thead>
<tr>
<th>Scorecards</th>
<th>Tables</th>
<th>Views</th>
<th>Diagrams</th>
<th>Graphs</th>
<th>Globals</th>
<th>Time Periods</th>
<th>Back</th>
<th>Forward</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Failure: Hardware Failure KRI View, Score: 711.11 (Demo_Bank_V3.2005)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retail Bank KRI Aggregated Score</td>
<td>Actual</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RB: Online Banking Sys Aggregated Score</td>
<td>2.76</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RB: Online Banking Sys: User Volume</td>
<td>1.36</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RB: Online Banking Sys: Total Utilised Capacity</td>
<td>5,300</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RB: Online Banking Sys: Hardware Age</td>
<td>73%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RB: Online Banking Sys: Stress Testing Results</td>
<td>26 months</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RB: Cheque Processing Sys Aggregated Score</td>
<td>8.34</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RB: Cheque Processing Sys: Total Utilised Capacity</td>
<td>5.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RB: Cheque Processing Sys: Stress Testing Results</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RB: Cheque Processing Sys: User Volume</td>
<td>1800</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RB: Cheque Processing Sys: Hardware Age</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RB: ATM Processing Sys Aggregated Score</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RB: ATM Processing Sys: User Volume</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RB: ATM Processing Sys: Total Utilised Capacity</td>
<td>8.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RB: ATM Processing Sys: Hardware Age</td>
<td>30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RB: ATM Processing Sys: Stress Testing Results</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commercial Bank KRI Aggregated Score</td>
<td>9.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Company confidential - for internal use only
KRI aggregation

SAS Risk Intelligence Portal

Risk Heat Map

Hardware Failure: Hardware Failure KRI View, Score: 711.11 (Demo_Bank_V3Feb2005)

KRI Aggregated Score

- Retail Bank KRI Aggregated Score
  - RB: Online Banking Sys Aggregated Score
    - RB: Online Banking Sys: User Volume
    - RB: Online Banking Sys: Total Utilised Capacity
    - RB: Online Banking Sys: Hardware Age
    - RB: Online Banking Sys: Stress Testing Results
  - RB: Cheque Processing Sys Aggregated Score
    - RB: Cheque Processing Sys: User Volume
    - RB: Cheque Processing Sys: Total Utilised Capacity
    - RB: Cheque Processing Sys: Hardware Age
    - RB: Cheque Processing Sys: Stress Testing Results
  - RB: ATM Processing Sys Aggregated Score
    - RB: ATM Processing Sys: User Volume
    - RB: ATM Processing Sys: Total Utilised Capacity
    - RB: ATM Processing Sys: Hardware Age
    - RB: ATM Processing Sys: Stress Testing Results

Scorecard: Commercial Bank KRI Aggregated Score

Microsoft Internet Explorer

The formula is: if((Retail Bank KRI Aggregated Score, RB: Cheque Processing Sys Aggregated Score, RB: Cheque Processing Sys: User Volume - Actual) > 3000) and ((Retail Bank KRI Aggregated Score, RB: Cheque Processing Sys Aggregated Score, RB: Cheque Processing Sys: Total Utilised Capacity - Actual) > 60) and ((Retail Bank KRI Aggregated Score, RB: Cheque Processing Sys Aggregated Score, RB: Cheque Processing Sys: Hardware Age - Actual) > 36) and ((Retail Bank KRI Aggregated Score, RB: Cheque Processing Sys Aggregated Score, RB: Cheque Processing Sys: Stress Testing Results - Actual) > 4, 1, 0)

OK
Diagnostics and drill down functionality

<table>
<thead>
<tr>
<th>Parent Link</th>
<th>Description</th>
<th>Update Frequency</th>
<th>Source System</th>
<th>Unit of Measurement</th>
<th>Red Threshold</th>
<th>Amber Threshold</th>
<th>Green Threshold</th>
<th>Forecast</th>
</tr>
</thead>
</table>
Analytics & Trend analysis

Forecast for Users utilising Online Banking Sys in Retail Bank

Generated by SAS OpRisk Solution
KRI's Monitoring - Users utilising Business Systems

Generated by SAS OpRisk Solution
### Controls and Action Plan Details

<table>
<thead>
<tr>
<th>Controls</th>
<th>Current Control Effectiveness Score (1-9)</th>
<th>Action Plan</th>
<th>Completion Date</th>
<th>Completion Status (%age)</th>
<th>Action Plan Owner</th>
<th>Target Control Effectiveness Score (1-9)</th>
<th>Cost of Action Plan (£)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation procedure to be performed only by installers trained and certified by equipment supplier.</td>
<td>2</td>
<td>Include certification training in the personal development plan for all staff</td>
<td>20/FEB/2005</td>
<td>80.00%</td>
<td>Jean Coombes</td>
<td>7</td>
<td>880,000</td>
</tr>
</tbody>
</table>

Country = UK

Control = Installation procedure to be performed only by installers trained and certified by equipment supplier.
## Populating the risk map

<table>
<thead>
<tr>
<th>Capital Markets</th>
<th>Conduct</th>
<th>Process</th>
<th>External</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Origination</td>
<td>Litigation &amp; Complaints</td>
<td>Key Leavers</td>
<td>Damage to Physical Assets</td>
</tr>
<tr>
<td></td>
<td>Staff Disciplinary Cases</td>
<td>IT Downtimes</td>
<td>External Theft &amp; Fraud</td>
</tr>
<tr>
<td>Execution/Trading</td>
<td>Off Market Transactions Mis-marking</td>
<td>Trade Amends O/S Approvals</td>
<td></td>
</tr>
<tr>
<td>Risk Mgt</td>
<td></td>
<td>Limit Breaches</td>
<td>Defaults</td>
</tr>
<tr>
<td>Settlement/Processing</td>
<td>Unconfirmed Trades</td>
<td>Fails/Cash Breaks</td>
<td>ML Reports</td>
</tr>
<tr>
<td>Support</td>
<td></td>
<td></td>
<td>Audit Issues</td>
</tr>
</tbody>
</table>

### Internal
- Employment Practices & Workplace Safety
- Clients, Products, & Business Practices
- Internal Theft & Fraud
- Execution, Delivery, & Process Mgmt
- Business Disruption & System
- Failures
- Damage to System

### External
- Theft & Fraud
- BCP Callouts

---

*Copyright © 2003, SAS Institute Inc. All rights reserved.*

*Company confidential - for internal use only*
Central control over corporate KRI’s and data model

<table>
<thead>
<tr>
<th>Event Risk Categories, Event Risk Subcategories, Risk</th>
<th>Asset Management</th>
<th>Retail Brokerage</th>
<th>Corporate Finance</th>
<th>Trading and Sales</th>
<th>Agency Services</th>
<th>Payment and Settlement</th>
<th>Retail Banking</th>
<th>Private Banking</th>
<th>Core Bar</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Disruption and System Failures</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1,008,000</td>
<td>50,232,000</td>
<td>0</td>
<td>16</td>
</tr>
<tr>
<td>Clients, Products and Business Practices</td>
<td>497,400,000</td>
<td>399,000,000</td>
<td>224,000,000</td>
<td>552,760,000</td>
<td>273,200,000</td>
<td>52,400,000</td>
<td>595,800,000</td>
<td>64,800,000</td>
<td>6,648</td>
</tr>
<tr>
<td>Unauthorized Activities</td>
<td>59,500,000</td>
<td>16,000,000</td>
<td>0</td>
<td>151,600,000</td>
<td>803,000</td>
<td>1,600,000</td>
<td>16,800,000</td>
<td>4,800,000</td>
<td>2,0</td>
</tr>
<tr>
<td>R49: Conducting unauthorized transactions</td>
<td>54,900,000</td>
<td>16,000,000</td>
<td>0</td>
<td>101,600,000</td>
<td>320,000</td>
<td>1,600,000</td>
<td>16,800,000</td>
<td>4,800,000</td>
<td>2,0</td>
</tr>
<tr>
<td>Exceeding trading limit</td>
<td>4,800,000</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Improper Business Practices</td>
<td>66,400,000</td>
<td>168,400,000</td>
<td>125,200,000</td>
<td>345,760,000</td>
<td>15,600,000</td>
<td>13,800,000</td>
<td>257,400,000</td>
<td>15,200,000</td>
<td>4,400</td>
</tr>
<tr>
<td>Improper Sales or Client Practices</td>
<td>371,400,000</td>
<td>153,600,000</td>
<td>33,600,000</td>
<td>205,400,000</td>
<td>255,800,000</td>
<td>30,000,000</td>
<td>319,600,000</td>
<td>64,800,000</td>
<td>24</td>
</tr>
<tr>
<td>Damage to Physical Assets</td>
<td>25,200,000</td>
<td>1,200,000</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Employment Practices and Workplace Safety</td>
<td>11,200,000</td>
<td>32,500,000</td>
<td>8,400,000</td>
<td>7,200,000</td>
<td>0</td>
<td>0</td>
<td>33,400,000</td>
<td>1,200,000</td>
<td>26</td>
</tr>
<tr>
<td>Execution, Delivery and Process Management</td>
<td>2,000,000</td>
<td>800,000</td>
<td>3,200,000</td>
<td>50,400,000</td>
<td>20,400,000</td>
<td>3,600,000</td>
<td>124,000,000</td>
<td>600,000</td>
<td>14</td>
</tr>
<tr>
<td>External Fraud</td>
<td>64,000,000</td>
<td>38,000,000</td>
<td>37,600,000</td>
<td>22,800,000</td>
<td>259,000,000</td>
<td>5,600,000</td>
<td>51,200,000</td>
<td>62,000,000</td>
<td>35</td>
</tr>
<tr>
<td>Internal Fraud</td>
<td>0</td>
<td>3,200,000</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>55,600,000</td>
<td>0</td>
<td>800,000</td>
<td>2,4</td>
</tr>
</tbody>
</table>
**Risk monitoring including KRI’s**

---

**Global: Risk (Demo_Bank_v2.Feb2005)**

<table>
<thead>
<tr>
<th>EventRiskSubCategories</th>
<th>System Functions</th>
<th>EventRiskCategories</th>
<th>Business Disruption and System Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description**

All system failures caused by hardware failures. Some examples include insufficient disk space, corrupt failed memory etc.

**Owner**

Keith Evans

Email: keith.evans@europeanbank.com

Work Phone: +44 (0) 222 8899

**Risk and Controls**

Control for Hardware Failure

Control Details:


**KRI’s**

Hardware Failure KRI’s

KRI Detail:


**Internal Losses**

Internal Losses for Hardware Failure

Internal Loss Detail:

Drilldown capabilities to identify potential issues.

<table>
<thead>
<tr>
<th>Key Metric Aggregation</th>
<th>Global</th>
<th>Retail Bank</th>
<th>Commercial Bank</th>
<th>Asset Management</th>
<th>Card Services</th>
<th>Insurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Effective Controls</td>
<td>111</td>
<td>113.69</td>
<td>107.69</td>
<td>149.06</td>
<td>110.75</td>
<td>91.35</td>
</tr>
<tr>
<td>Number of Ineffective Controls</td>
<td>111</td>
<td>126.09</td>
<td>122.22</td>
<td>76.47</td>
<td>83.33</td>
<td>152.53</td>
</tr>
<tr>
<td>Total OpRisk Losses (£)</td>
<td>107</td>
<td>146.74</td>
<td>86.86</td>
<td>75.77</td>
<td>162.76</td>
<td>92.31</td>
</tr>
<tr>
<td>Number of OpRisk Loss Events</td>
<td>105</td>
<td>76.47</td>
<td>133.33</td>
<td>77.78</td>
<td>141.18</td>
<td>114.81</td>
</tr>
<tr>
<td>Number of Business units submitting loss data</td>
<td>126</td>
<td>133.33</td>
<td>75.00</td>
<td>125.00</td>
<td>155.56</td>
<td>127.50</td>
</tr>
<tr>
<td>Total External OpRisk Losses (£)</td>
<td>103</td>
<td>77.40</td>
<td>98.95</td>
<td>75.77</td>
<td>162.76</td>
<td>92.31</td>
</tr>
<tr>
<td>Number of External OpRisk Loss Events</td>
<td>109</td>
<td>78.82</td>
<td>130.51</td>
<td>80.56</td>
<td>141.43</td>
<td>110.71</td>
</tr>
<tr>
<td>Number of Risk Assessment questionnaires in latest Self Assessment exercise</td>
<td>112</td>
<td>128.57</td>
<td>116.00</td>
<td>106.90</td>
<td>118.75</td>
<td>90.00</td>
</tr>
<tr>
<td>Internal fraud related losses</td>
<td>117</td>
<td>106.91</td>
<td>27.99</td>
<td>107.05</td>
<td>440.02</td>
<td>73.55</td>
</tr>
<tr>
<td>External fraud related losses</td>
<td>99</td>
<td>139.93</td>
<td>157.21</td>
<td>42.63</td>
<td>164.07</td>
<td>105.27</td>
</tr>
<tr>
<td>Staff turnover (%)</td>
<td>122</td>
<td>84.00</td>
<td>54.00</td>
<td>109.09</td>
<td>138.52</td>
<td>95.68</td>
</tr>
<tr>
<td>Number of Risk and Control related Issues</td>
<td>120</td>
<td>85.19</td>
<td>175.00</td>
<td>69.23</td>
<td>338.46</td>
<td>79.17</td>
</tr>
<tr>
<td>Number of Action Plans behind planned date</td>
<td>68</td>
<td>166.67</td>
<td>66.67</td>
<td>50.00</td>
<td>50.00</td>
<td>40.00</td>
</tr>
</tbody>
</table>
View KRI linked with Business Process or Risks
Root cause analysis embedded into the data model

Dashboard

Causes

- Preventive actions not taken to resolve the weaknesses highlighted in the quarterly stress testing process.
- Marketing failed to inform IS team about the Christmas credit card campaign.
- New disk space added to the system not installed correctly.

Risk Event

Hardware Failure: System running the online banking system of the retail bank was taken off line. The system was unable to cope with increased user traffic on the website and had to be taken offline to resolve the problem.

Loss

- Overtime paid to IS staff to stay in office to resolve the problem.
- Increased volume of incoming calls to customer support call center as customers unable to perform transactions on the online website.
- Compensation to customers whose transactions could not be processed and requested compensation from the bank.
- Unable to process customer direct debit.
- Press coverage in FT and Wall Street Journal.

Business Unit

- Information Systems
- Customer Support Call Center
- Online Banking
- Marketing
Coherent information based on a fully integrated system
Conclusion

Key Risk Indicators are a core component of any OR management programme –

• to establish basic transparency and reporting obligations
• to build best practice both internally and industry-wide
• to implement bottom-up disciplines for risk cost-benefit
• as scalars for historical internal or external loss data
• as capital drivers and incentive mechanisms for risk mgt

A KRI programme is not a pure data exercise … it is ultimately about managing issues and actions, and changing behaviour
In Conclusion...

...KRIIs are about managing effective organizations...

...an effective KRI framework is based on a sophisticated evolving system to reflect business environment changes...
Implementing a KRI program

How KRIs help the business...

- Promote dialogue on people, technology, and process inefficiency;
- Take a proactive approach to managing risk
- Enable management to take mitigating actions;
- Enable performance comparison between business functions
- Improve resource allocation across the business line or, more globally, across an enterprise or region

Benefits
Implementing a KRI program

How KRIs help the enterprise...

- Develop trending information and establish trends
- Develop and disseminate best practices for risk mitigation
- Establish risk metrics aligned to risk appetite and performance management
- Better strategic decision based on coherent view of risks