The Management Consultants.

CHALLENGES IN THE QUANTIFICATION OF OPERATIONAL RISK

RiskLab-Madrid

Madrid, 14. November 2002

IBM Unternehmensberatung GmbH

The Management Consultants.

Agenda

The Management Consultants.

Agenda

Senior Management would much easier acknowledge the high value of operational risk management, if one could deliver quantifications in the following areas:

Relevant questions:

- Can you help finding an efficient project portfolio?
- Can you support the business case of projects?
- Can you help assuring and afterwards assess the success of a project?
- Can you help in outsourcing decisions and implementations?

The smallest part of the effort to build and run an operational risk management is the developpment of VaR calculation models and engines.

Identify → Track → Measure → **Manage**

Identify

Identify and describe all potential process risks

Data Collection

Prioritisation of risks

Track

Find means to track risks

Create report mechanism

Measure

Assess the importance of the risk
- Risk probability
- Risk impact

Develop and continuous refinement of VaR calculation models

Manage

Integrate Oprisk exposure data in managment process

Manage Oprisk exposure(e.g. insurance)

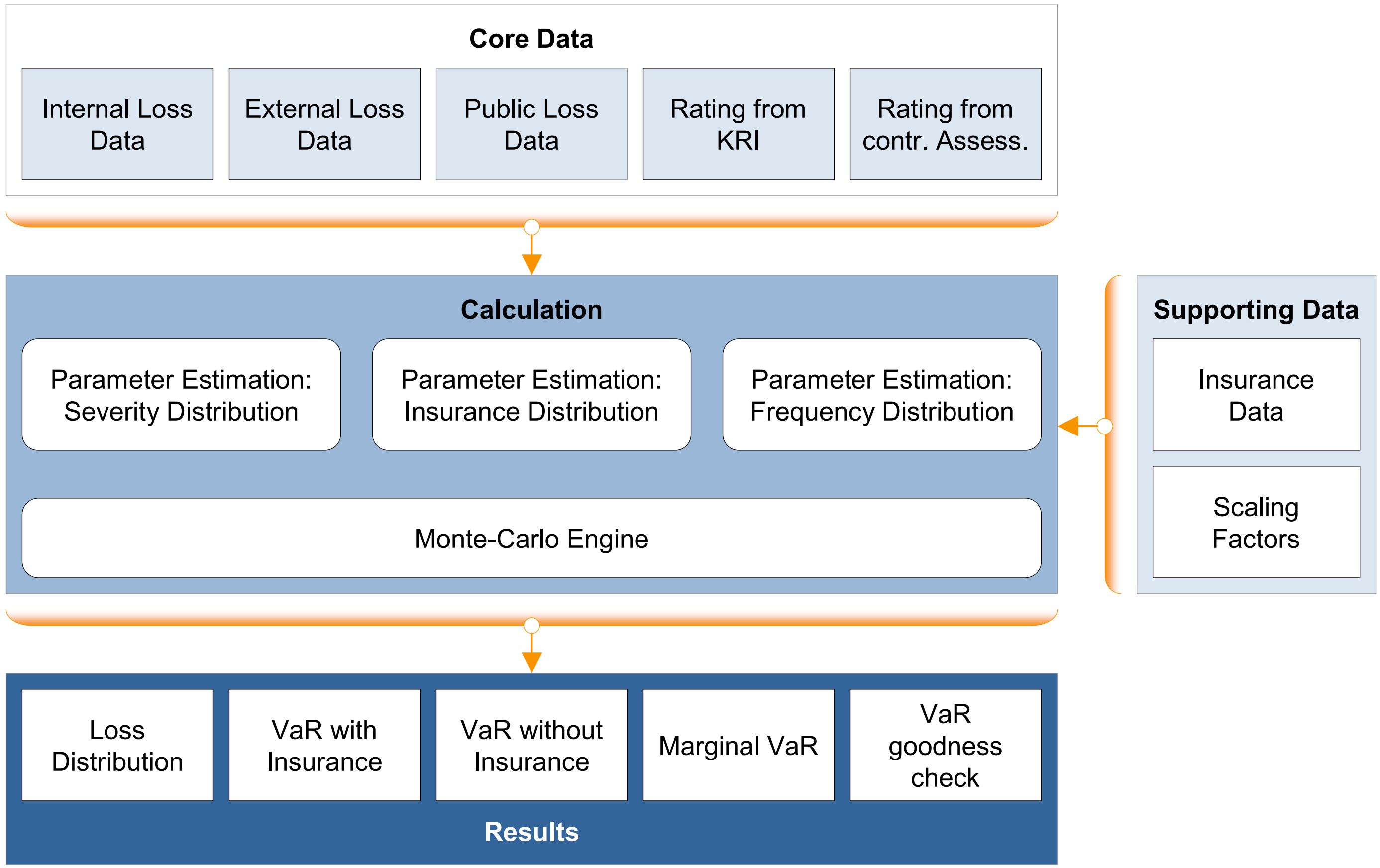
75%

5%

20%

Agenda

The core functionality of the operational risk VaR calculation is realized in routines for testing and demonstration



Severity Distribution

The severity parameter estimation is the most sensitive part of the parameter estimation and a method "toolbox" has to be available to cover different data types and availability condition .

Methods devised and prototyped:

- Maximum likelihood (MLE) fit to internal data

  6 different distribution types
  - Weibull
  - Burr
  - Expontential
  - Lognormal
  - Pareto
  - Gen. Pareto
- Minimum least square fit to data in histogram form
- Mixing of internal with external data
  - Integrated MLE
  - Sequential MLE
  - for equal or similar internal and external data
- Loss events series reconstruction from histograms

  (new method)
- Extreme Value Theory / Peaks over Thresholds

Frequncy Distribution

The estimation of the expected number of loss events "will" be done from the internal loss history, self assessment, key risk indicators and gross exposure indicators.

Methods devised:

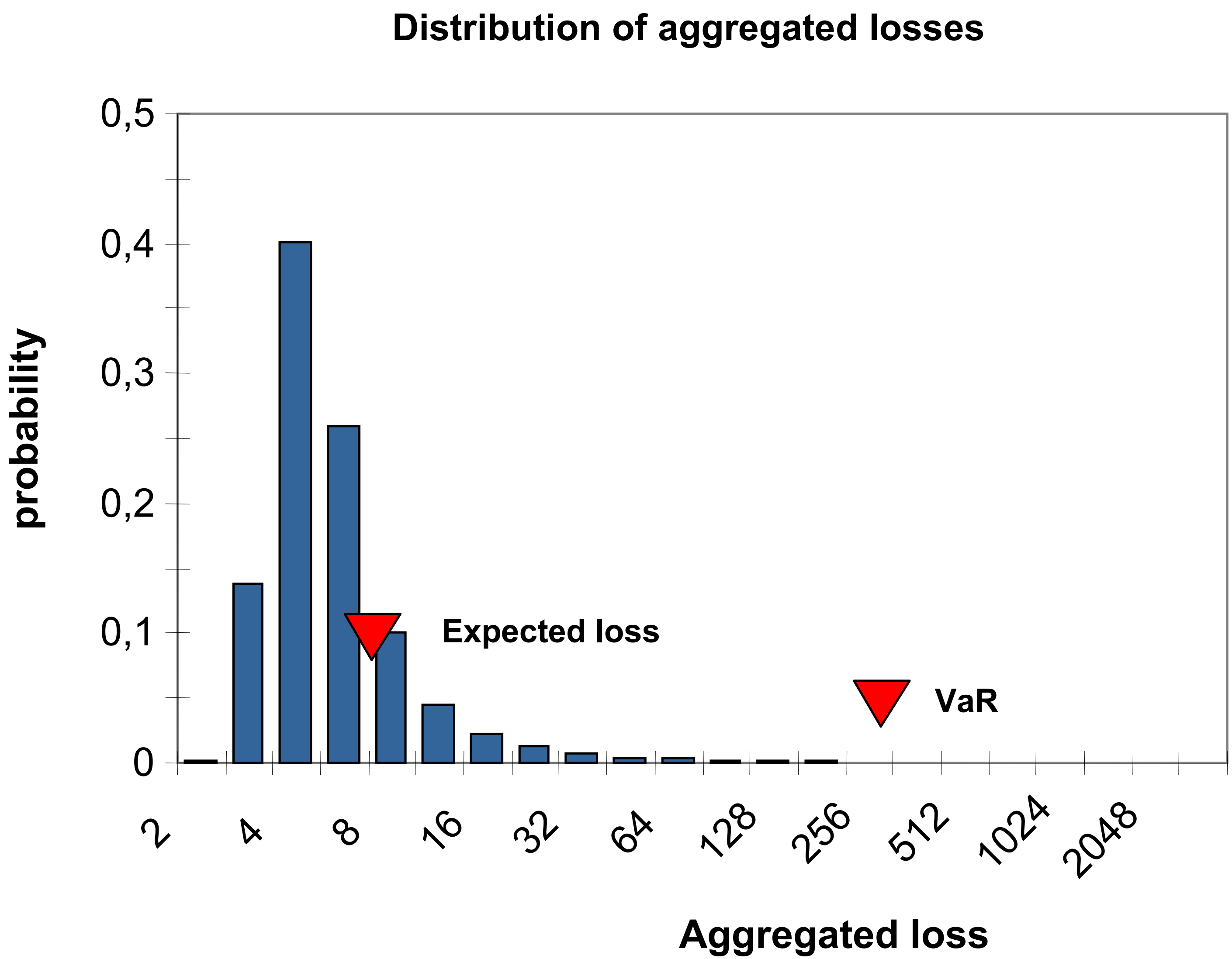
- Allow different distribution to account for different standard deviations of the frequency distribution
- Integrate the following data sources
  - Internal loss history
  - exposure indicators
  - self assessments
  - key risk indicators

Mathematical tools

- Maximum likelihood estimator
- Neural or Bayesian networks
- "Time series filter tools"

Monte-Carlo Engine

Based on the currently available loss data the Monte Carlo calculation calculates an expected loss of x and a Value at Risk of y.

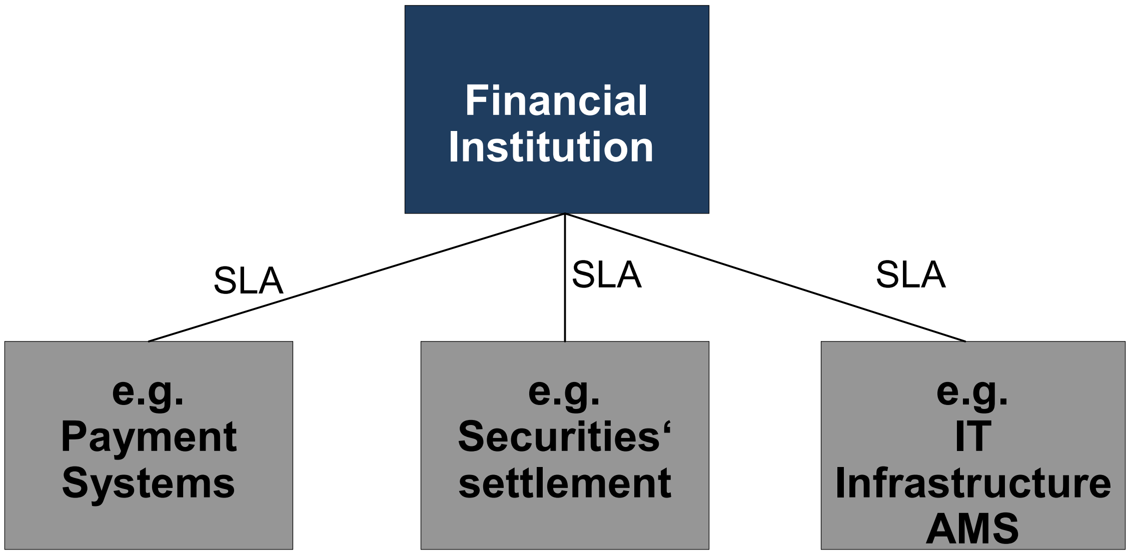


Agenda

The Business Case of outsourcing is strongly influenced by operational risk capital savings.

Quantification issues in the context of outsourcing

- Operational VaR before outsourcing
- Operational VaR after outsourcing
- Risk Transfer Pricing
- Pricing of penalties within Service Level Agreements



Examples for Outsourcing Areas of a Financial Institution

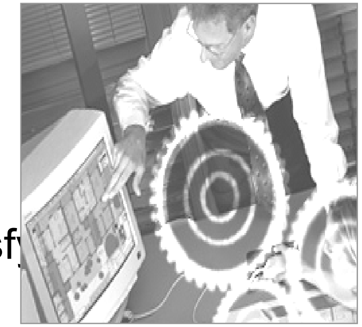
What are Service Level Agreements

Definition

- A Service Level Agreement includes an obligation between a customer a (external or internal) to support the needs of the customer to a defined le

Benefits

- Better/clearer communication between customer and provider
- Predictability of amount of service
- Consolidation of required services.
- Achievement of a consistent level of quality
- Guarantee that availability and performance of technical solutions satisf demands.



There are a range of important questions relevant for Service Level Agreements

Relevant questions

- How are Service Level Agreements (SLAs) incorporated into the existing contracts with banks.
- How homogeneous are the existing contracts
- To what extent are risk relevant issues integrated into the current SLAs?
- Can the existing SLAs be modified and/or adapted?
- Are the banks willing to pay for the new service?
- Or must the services be offered free in order to remain in the market?
- What possible pricing structures are available?
- How do you price penalties?
- In the case that the operational risk is passed on to a third party, what are the results?
- How should SLAs with a third party look like?

Risk transfer can only be achieved after a series of steps

Example

1

Selection of the relevant processes

- Not every process hides a relevant operational risk

2

Clear documentation of processes

- Particularly important are the interfaces and the transfer of responsiblity

3

Formalisation of criteria of measuring service

- Criteria should not only be meaningful, but also measurable

4

Establishment of a contolling/reporting system

The content of the SLA should be continuously monitored

5

Appropriate penalties agreed

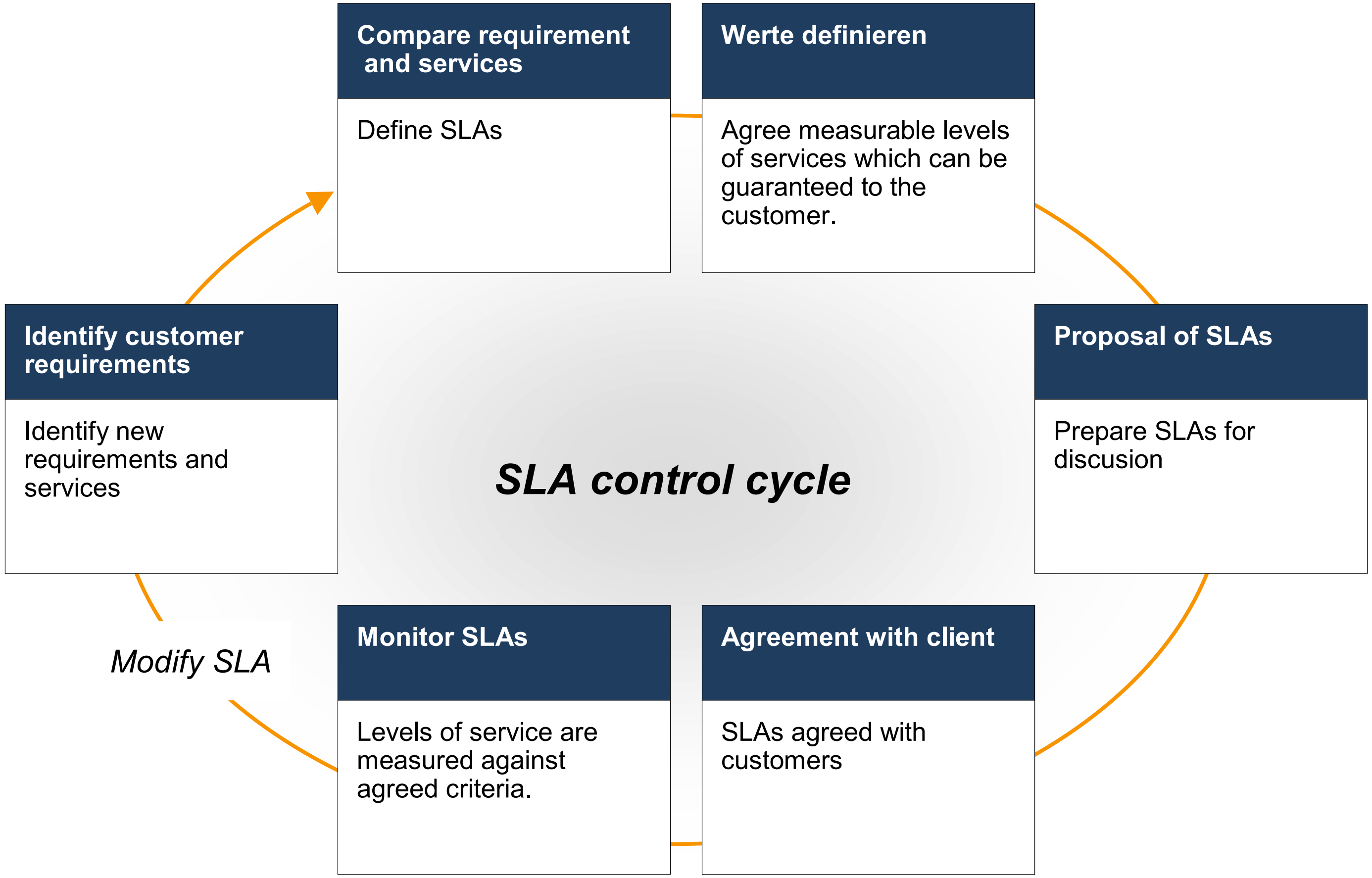
- Risks should be measured in terms of proability and costs.
- Each possible outrage should be formally documented
- One component of this is the financial cost of an outrage (with reference to expert knowledge)
- The penalties should be agreed and become part of the SLA

6

Regular control cycle

- SLAs should be regularly reconciled with business requirements

Service Level Agreements require regular tuning, otherwise, over the longterm, there is the risk that supply and demand diverge from one another.



The SLA controlling cycle ensures a continual improvement of the levels of service and and a regular integration of new customer requirements (and also elimination of no-longer-necessary services)

The identification, assessment and consolidation of operational risks, together with effective communications between the Operational Risk Managment (ORM) and the Line of Business (LoB) is the purpose of the risk mapping process.

Beispiel

The operational risk process is initially driven by the risk mapping workshop.
Here a group of experts identify and document all the relevant risks

Planning and Methodology for risk mapping workshops → **Communication between lines of business** → **Introduction of Results of workshop into live environment** → **Documentation of results** → **Reporting**

How can the operational risks of outsourcing be minimised? By the introduction of an appropriately prophylactic process

Analyse risks → Quantify risks → Manage risks → Monitor risks

The introduction process is classic risk managment:

Analyse risks

- Risks are identified as the result of a systematic analysis

Quantify risks

- The potential costs of identified risks can be assessed.

Manage risks

- There are a range of possibilities, from internal risk mangement to risk transfer to a third party (insurance).

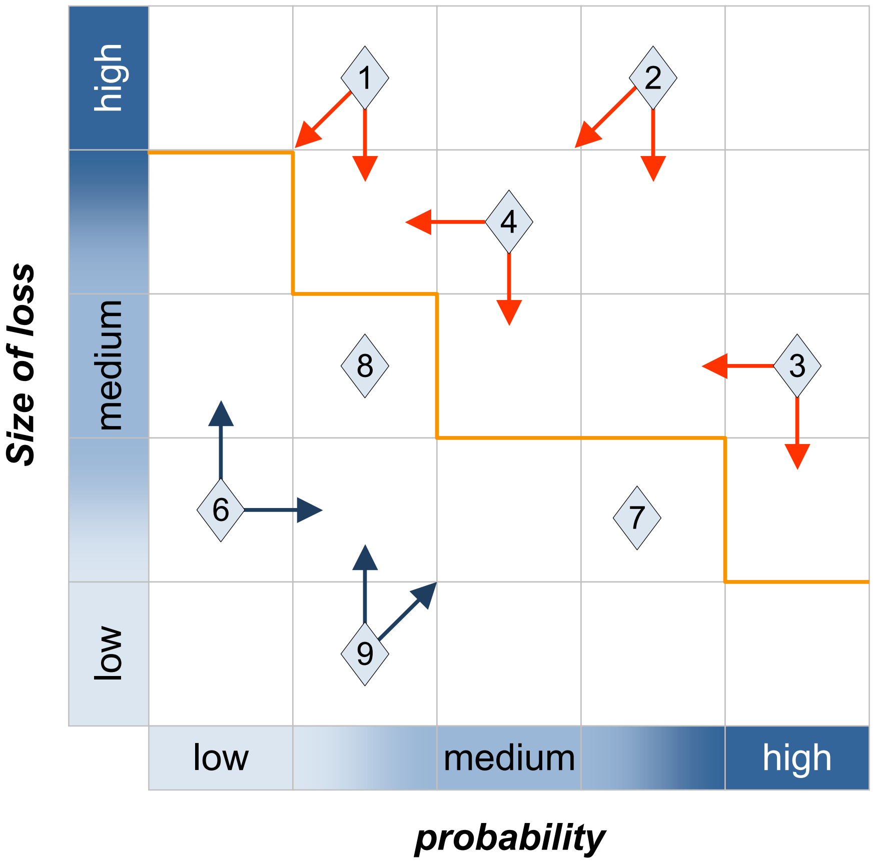
Monitor risks

- The set of potential risks should be continuously monitored both to assess the efficiency of the risk management regime, and to ensure that new risks are analysed and taken up as soon as they appear.

The Management Consultants.

Agenda

The introduction of operational risk managment factors into management decisions not only allows investment to be better managed, but also savings in ‘over-secure’ areas.



Presentation of risks at the level of the company or business unit.

- Identify acceptable risks
- Aggregation per business area, process step, or risk category
- Focussed risk reduction ***and*** focussed acceptance of higher risks (taking into account control measures, reduced availability etc.)
- Efficient mangement of of investments
- Finally: limiting of cumulative risk (capital reserves)

Risk acceptance-boundary (for single risks)

Risk estimate for an area (risk category,, business area, etc.)

Infrastructure projects are often justified by the reduction of operational risk. However in order to be able to calculate a break even of such an investment you need to be able to quantify operational risk.

Top Down view

Estimated savings on capital reserves as a result of reduction of operational risks*	In €M
Tier I + II reserves ABC-Bank	8.000
Of which operational risk component	15%
Capital reserves for operational risks	1.200
Of which percent for operational risk in treasury business	25%
Capital reserves for operational risks in treasury business	300
Of which savings as a result of new goal architecture (conservative estimate)	15%
Interest on capital reserves	6,25% p.a.
Resulting savings on reserves costs as a result of new architecture	**2,8 p.a.**

Bottom Up view

Examples from the banking world of losses stemming from problems in operations

Allied Irish Bank (large loss/rare event)
Fraud in treasury department of US-daughter firm Allfirst cost the group $750M (2001).

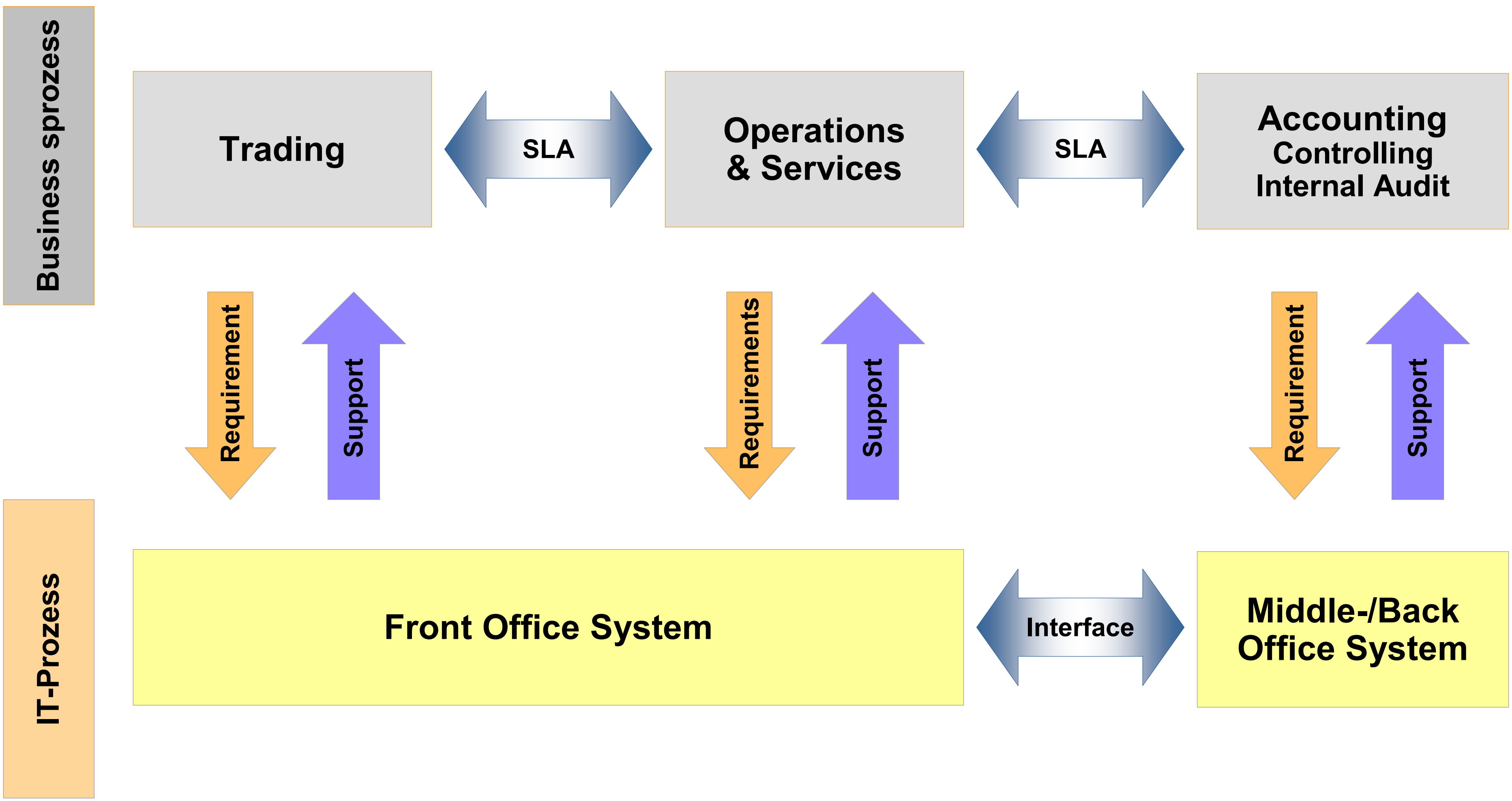
Daiwa Bank (large loss/rare event)
Criminal cover-up of $1.1 billion of trading losses. Regulatory fines $ 340 million (1984-1995)

Medium sized loss/common event
- Errors in position reporting as a result of inadequate processes: Loss ca 0,8 Mio Euro, occurrence ca. 10/Yr.
- false management of turnover as a result of inadequate processes: Loss ca 0,05 Mio Euro, occurance ca. 1/day

** Extracted from Quantitative Impact Study 2002*

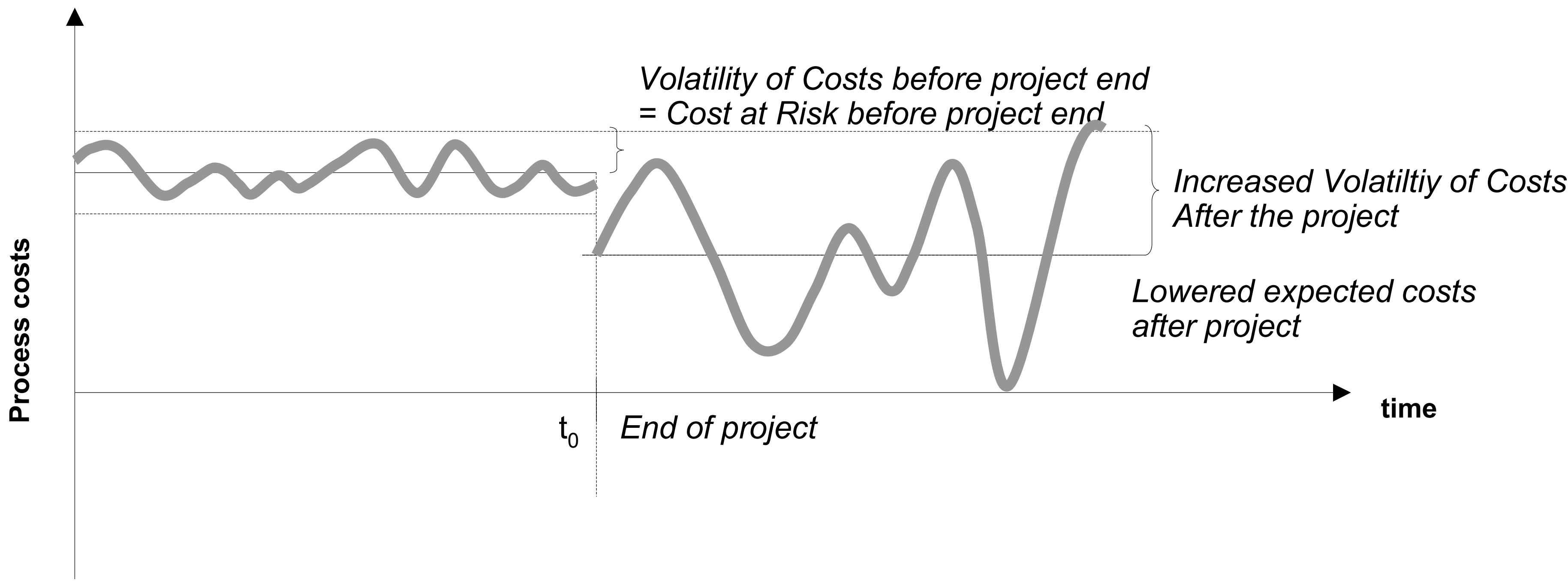
You need to incorporate operational risk trackings into the project in order to assure the operational risk reduction. Observing the reduction of losses after completing the project should decide about the success of the project.

Example Derivates business



Cost cutting projects usually reduce „expected costs“. Including „unexpected costs“ might change the business case.

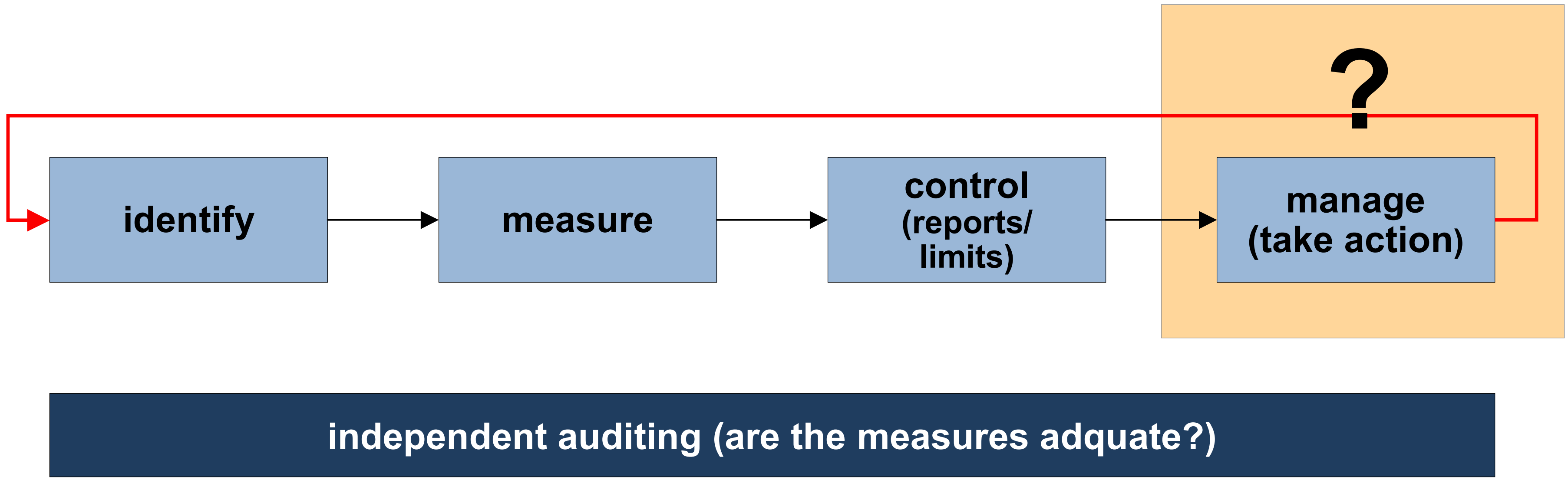
Danger of increasing „unexpected costs“



Agenda

The Management Consultants.

Risk management can only be successful when management level decisions are made on the basis of the numbers delivered by the risk management process



Investment decision