Finanzgruppe
Deutscher Sparkassen- und Giroverband

How to Gain Value from Scenario Analysis And Data Pooling

Practical Techniques for the Management And Measurement of Operational Risk

Bank for International Settlements, Basel, October 24-26, 2006

Dr. Johannes Voit

Structure of the German Savings Banks Network

- 690 corporations under the umbrella of the German Savings Banks and Giro Association; most corporations under public law
- Financial network consisting of
  - 463 Savings Banks with balance sheet sizes from 100 Mill. € to 40 Bill. €
  - 11 Landesbanken (Federal states' banks)
  - 37 public insurance companies
  - 11 mortgage banks
  - many partners for leasing, factoring, EDP services, investment funds, publishing …
  - 11 regional and 1 national association (DSGV)

Why Scenario Analysis?

- Know your risk (not the loss history)
  - Not enough losses
  - Possibly no losses at all
- Seeing tomorrow
- Uses knowledge of staff
- “What … - if …” thinking drives management action
- Prioritize possible management action, e.g. by re-evaluating scenario after implementation
- Pillar 2 implementation may require scenario analysis (p. ex. Germany)
- EU CRD requires scenario analysis in AMA

My Points Today

1. Practical implementations and best practice in scenario analysis
2. Developing credible scenarios
3. How to set up and successfully operate a data pool
4. Scenarios, pool data, and capital calculations: cornerstone or afterthought?
5. Using scenarios and pool data to drive process improvements

Finanzgruppe
Deutscher Sparkassen- und Giroverband

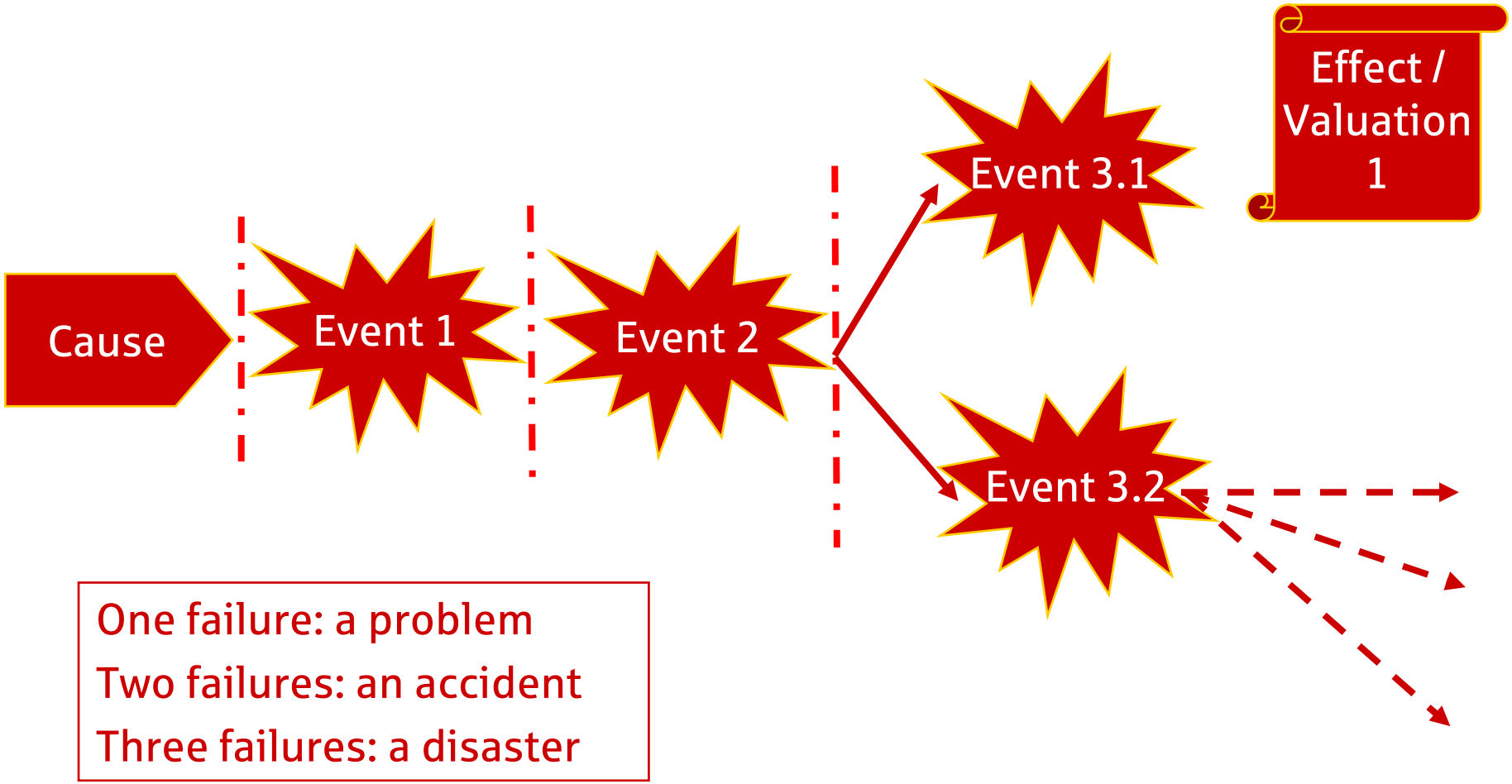
Practical Approaches to Scenario Analysis And Best Practices

What Is a Scenario?

A scenario is a chain of cause → effect → event

Cause	→	Due to an error,
Event	→	a transaction is entered incorrectly into the order system (e.g. wrong number of units, ticker symbol, or buy order instead of sell order). The client notifies the error after markets move against his position. She/he claims compensation of damage.
Effect	→	The savings bank agrees to pay a compensation

Chain Reaction / Tree Scenario: One Event Is the Cause of Another Event

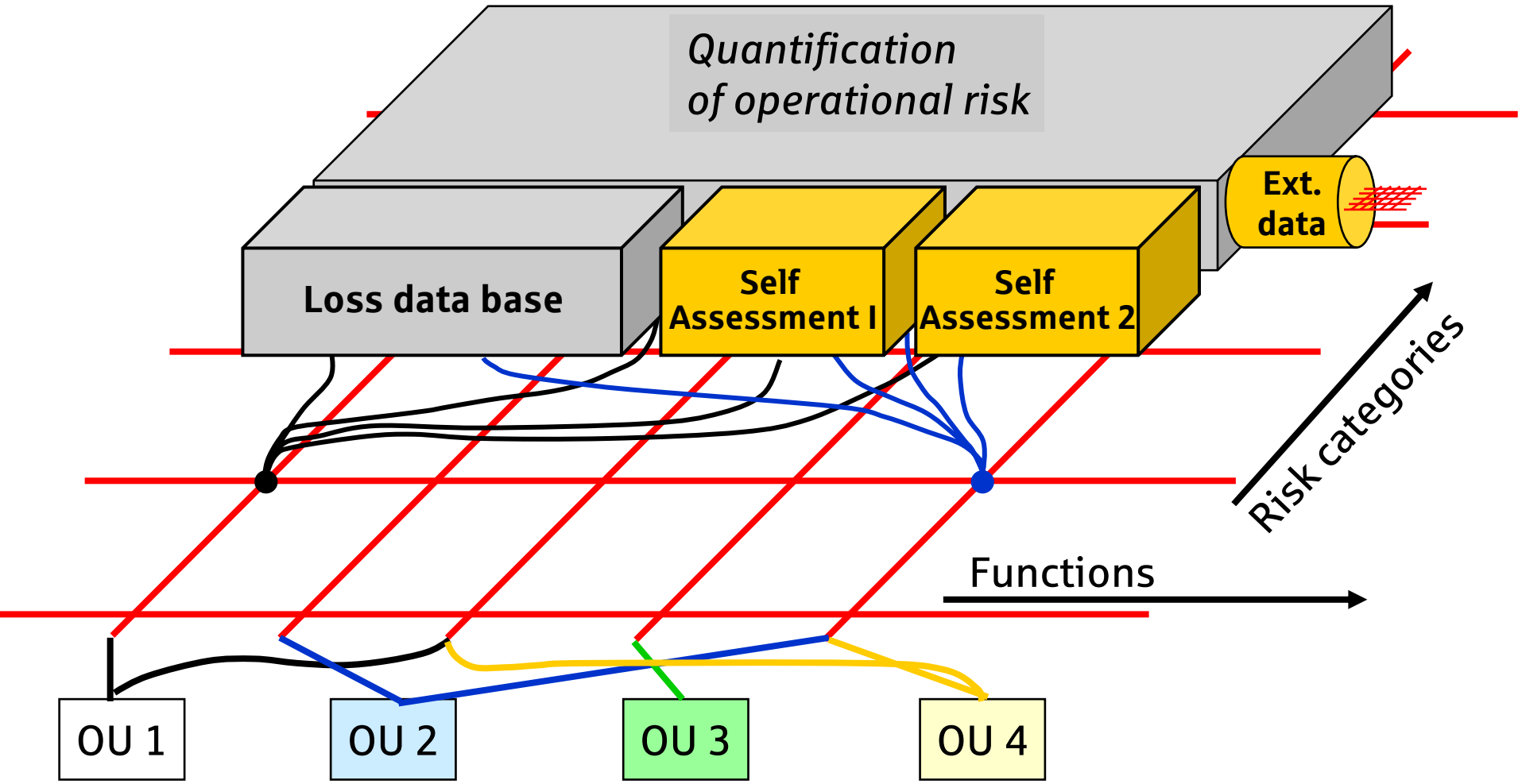


One failure: a problem
Two failures: an accident
Three failures: a disaster

The Complexity of the Valuation Depends on the Complexity of Your Model

- Standard Model of actuarial science
  - One frequency parameter (e.g. expected frequency)
  - Two severity parameters (e.g. mean and quantile)
- More complicated functions (2 parameters for frequency, 3 parameters for severity) possible, likely too difficult for assessors
- Ideal especially for validation by loss data:
  Break up valuation in loss components
  - Out-of-pocket expenses
  - Opportunity
  - Internal costs

Risk Categories And Functions Provide Permanent Backbone of Data Structure, And Connect All Instruments



Ensuring Scenario Quality Is a Laborious And Time-Consuming Task

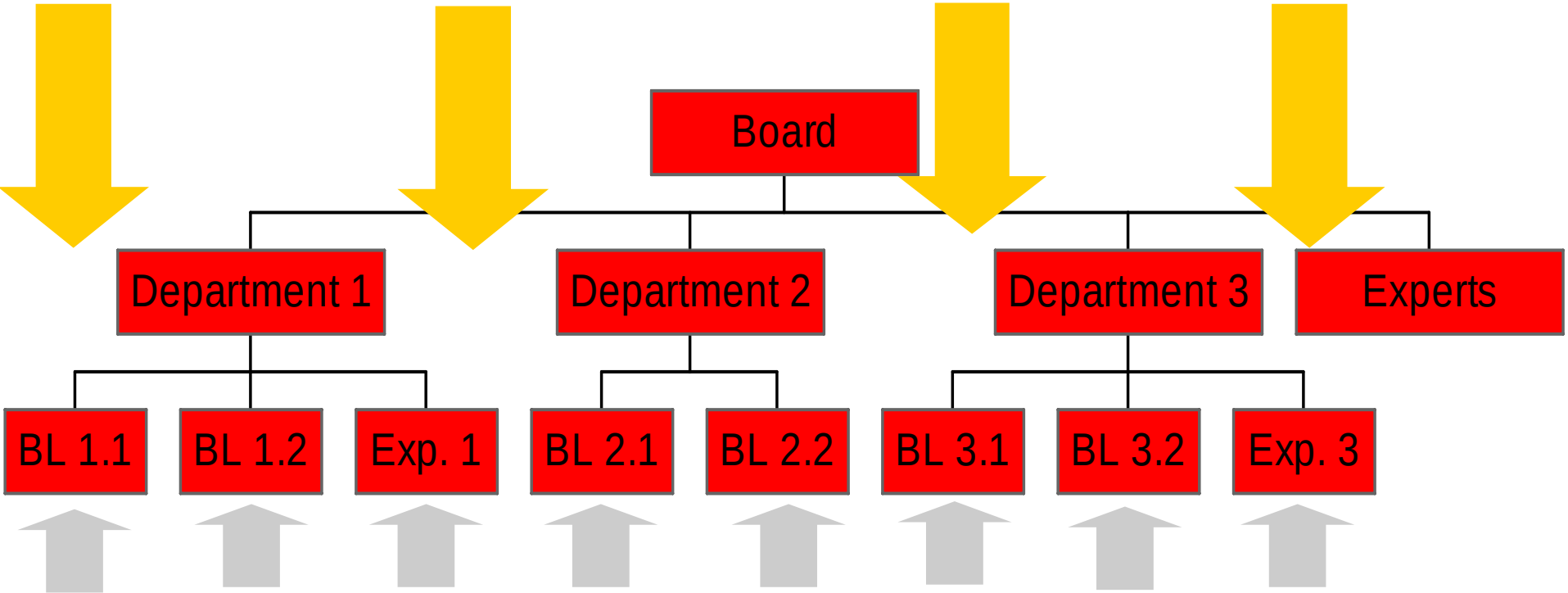
- Fears of making estimates / wrong estimates: Soft factors matter
- Understanding / formulating a scenario, making estimates is time consuming: use internal/external loss data and involve experts
- Quantities asked for must be transparent to assessor (often even “probability/frequency of an event” are NOT)
- Quantiles asked for should be within horizon of experience – but our experience shows that people more often than not tend to estimate rather high quantiles when thinking of “worst cases”
- Identifying “99.9% CL = 1 event / 1000 yr.” is not helpful
- Valuation must become transparent to a third person. This requires a meaningful description and a brief breakdown of the valuation scheme by the assessor

Coping with Subjectivity

- Validation (e.g. by loss history) sometimes possible but time consuming, assessor should be part of validation
- Cross checks possible even during/after interview: “Is this roughly what you mean?”
  - Sum of all frequencies
  - Simulate time series implied by an estimate under discussion
- Step-by-step validation
  1. Losses yes/no? Expected?
  2. Frequencies, average loss consistent?
  3. Quantiles/distributions consistent?
- Long, iterative process
- “Subjective” is not synonymous to “unreliable”

A Complete Overview Is Provided by a Combination of Bottom-Up And Top-Down Scenario Analysis

Quantitative exposure estimates: Focus top-down self assessment on **corporate risks** when combined with bottom-up SA



(Bottom up) self assessment:
Internal view of business lines
Quantitative exposure estimates [PE, ∅LGE, $q_{.99}$(LGE)]

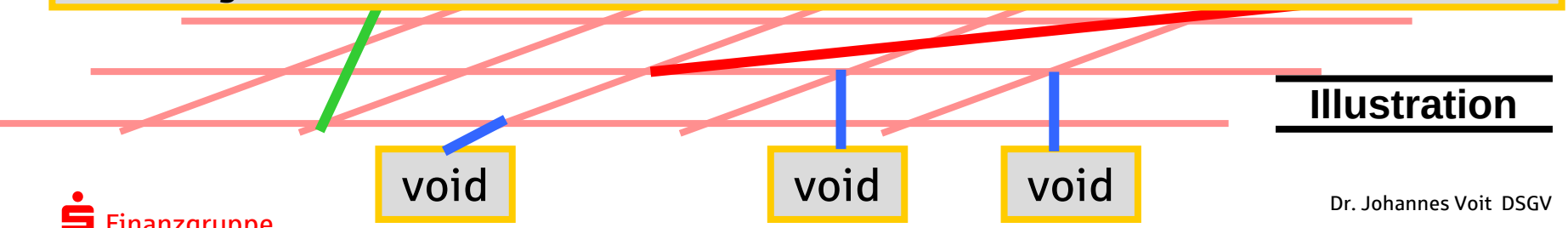
A Practical Bottom-Up Implementation Emphasizes Important Scenarios And Neglects Minor Ones

Due to too severe regulation for IT access, users do not log off after work. As a consequence, unauthorized data access and transactions take place. The savings bank suffers losses from the fraudulent transactions.

Frequency p. a.	0.2
Average loss per event, TEUR	35
99%-quantile of loss-given-event distribution, TEUR	4,000

Due to an error, a transaction is entered incorrectly into the order system. The client notifies the error after markets move against his position. She/he claims compensation of damage.

Frequency p. a.	3
Average loss per event, TEUR	5
99%-quantile of loss-given-event distribution, TEUR	80

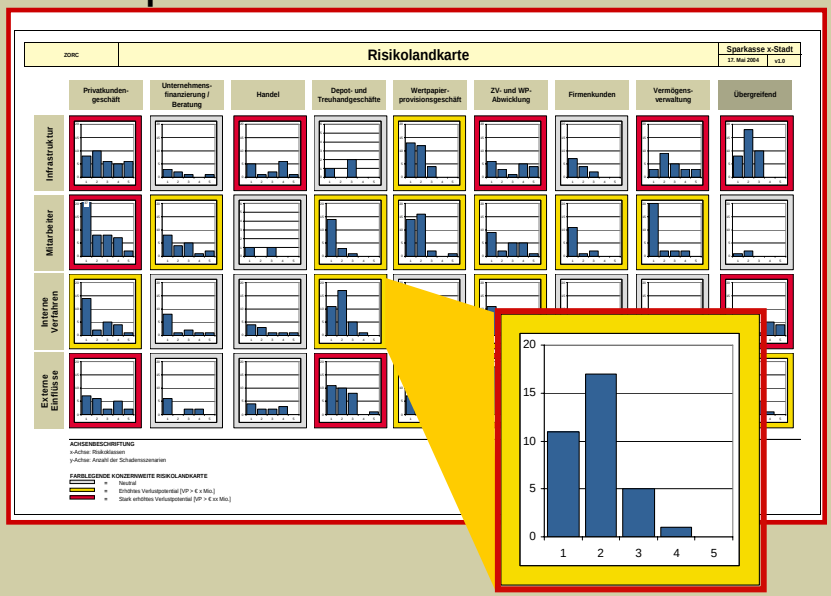


Illustration

Workshop-Based Top-Down Scenario Analysis Gives a Quick Overview of the Essential Risks of the Bank

- Workshop for senior management
- Estimate exposures for first level of risk category and functions only (simplification)
- Can be focused on important scenarios only
- Limited cost of implementation
- Annual update recommended

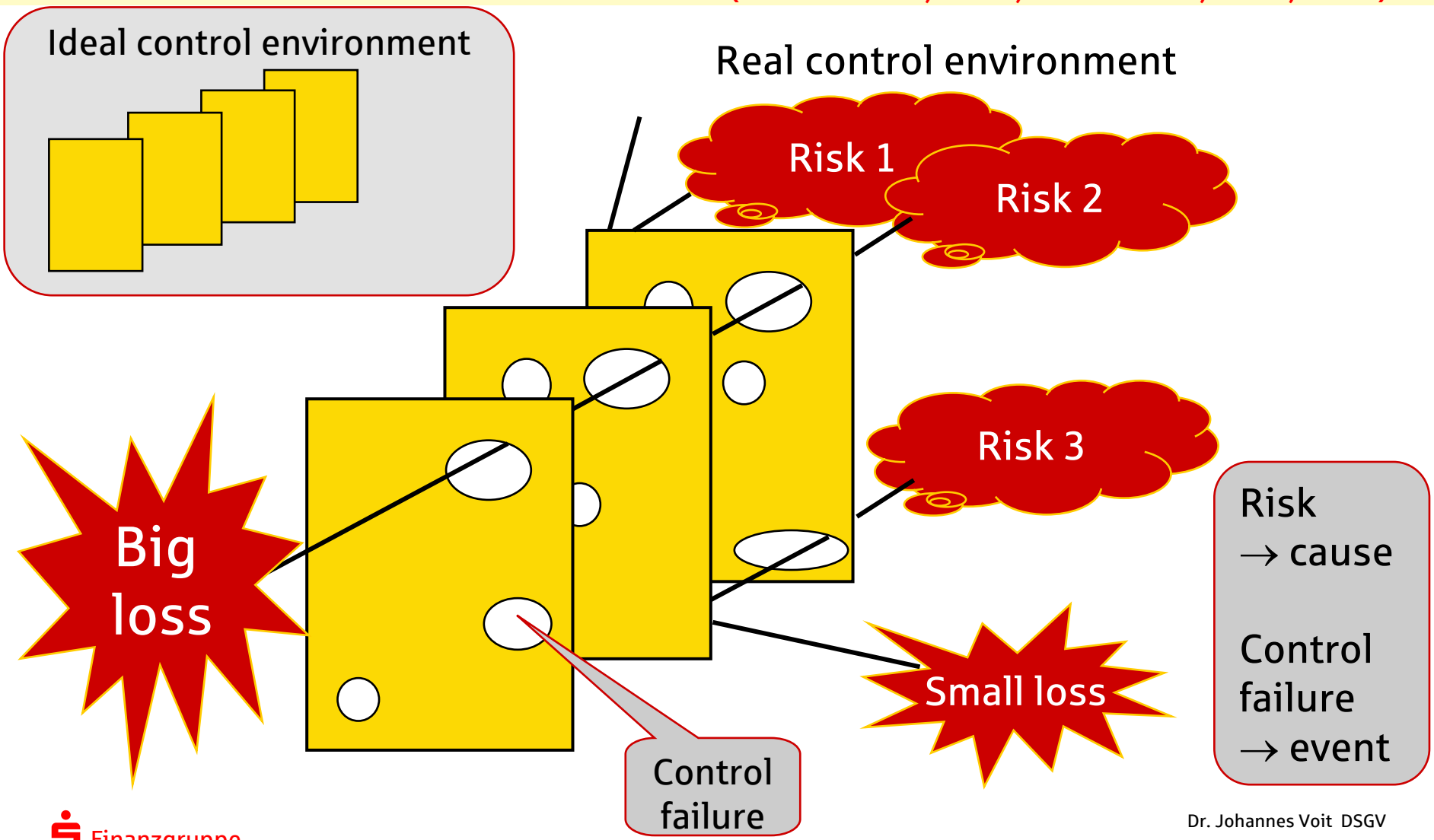
Example



- Identify business lines with large OR exposures (red) based on number and exposure of scenarios considered
- Drill down in selected areas or discuss appropriate action

Best Practice for Analysis Focused on Low-Frequency High-Severity Scenarios Is the Swiss Cheese Model

(after Reason, 1997, and J. Elder, CSFB, 2005)



Finanzgruppe
Deutscher Sparkassen- und Giroverband

Developing Credible Scenarios

Credible Scenarios Cannot Be Written Behind Closed Doors

- Credible means that the others are willing to buy into the scenario.
- Involve them into scenario formulation – either from the outset or in a review
- Select the most credible / important / plausible ones for evaluation. By comparing, people usually get a good feeling of what is important and what is not
- Connect to real cases, also from other sectors (insurance, police)
- Use all available information sources
  - Internal losses, documentation of near misses
  - External losses (data pools, ORX, Fitch/Algo FIRST, etc.)
  - External scenarios

- If you are unsure about the credibility of scenarios, consider discussing them with media people, journalists, etc.

A Very Specific Chain Reaction Scenario

On the afternoon of September 1, 2006, savings bank X is victim of a robbery. 25,000 € in cash were robbed. When fleeing, the gangsters damaged the locks of the two main entrance doors (outside to ATM area, ATM area to main hall). In order to protect its entrance, the bank hired a security service which provided a guard with a dog. In the evening, a new client of the bank entered the ATM area to withdraw money. (The client was acquired recently from a competitor and was considered a high-worth client). In a moment of inattention, the leashed dog escaped from the guard, attacked the client and bit his leg. The client was hospitalized for a few days. He claimed a compensation from the savings bank and threatened the bank to cut the newly established business relationship.

Good Scenarios Must Be Credible – But There Is More to Them!

- "It's so realistic – it must be the description of an actual loss event"

- This is a credible scenario – but is it a good one?
- None of the "simple", "generic", "plausible" scenarios
- Scenario easy to understand

- It is a very detailed / narrow scenario. As a consequence,
  - it is very rare,
  - there must be a lot of similar scenarios

Generalizing a Very Specific Scenario

On the afternoon of September 1, 2006, savings bank X is victim of a robbery. 25,000 € in cash were robbed.

Q: Should we limit ourselves to scenarios involving robberies? A similar story could also be developed, e.g., for a fire or flooding.

When fleeing, the gangsters damaged the locks of the two main entrance doors (outside to ATM area, ATM area to main hall).

Q: Other evolution of the story conceivable, e.g. crash the doors with a car, shootings, etc.

In order to protect its entrance, the bank hired a security service which provided a guard with a dog. …

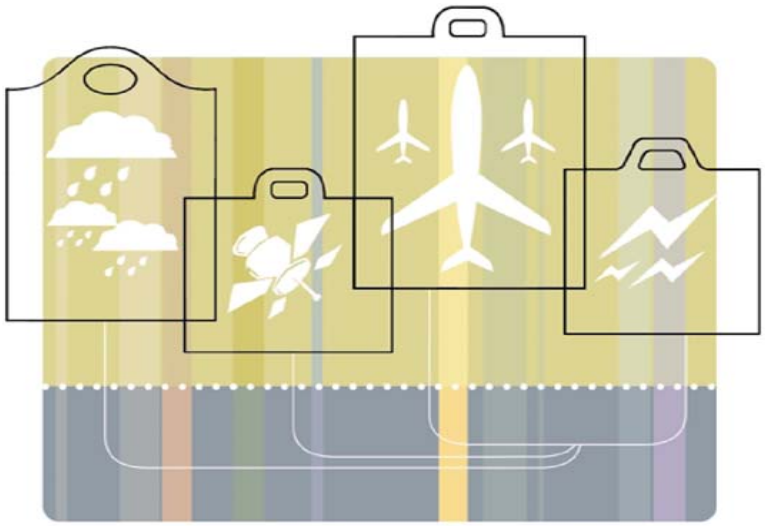
How to Make This Scenario a Good Scenario

- Use more general terms everywhere to cover broader situations: scenario will become abstract, difficult to understand, uninspiring

- Leave scenario unchanged but append instructions, e.g.
  - Please consider other external origins (fire, flood, earthquake, …) which may leave the savings bank in an insecure state, allowing a similar evolution of the scenario
  - Please consider other evolutions after the robberies (resp. alternatives) which cause further losses to the savings bank (e.g. burglary, damage to persons passing by, etc.)
  - When in conflict with risk categories, consider splitting the scenario.
  - When evaluating the scenario, please include the basic one-step scenario (e.g. no evolution after the robbery).

At Present, there Are No Worst Case Benchmark Scenarios Available for Banks

REALISTIC DISASTER SCENARIOS



Guidance and Instructions
April 2004

LLOYD'S

17 TERRORISM

Syndicates should complete both of the following hypothetical terrorist attack scenarios:

TRIA Event (covered by Terrorism Risk Insurance Act 2002)

The Midtown Manhattan area, New York, at 11:00am on 1 April 2004 suffers a 2-tonne bomb blast attack causing:

Zone	Impact Description	Damage Zones	Property Damage	Fire Loss
1	Collapse and fire following	Inner zone, radius 200m	100%	10%
2	Massive debris damage to surrounding properties	400m radius	25%	2.5%
3	Light debris damage to surrounding properties	500m radius	10%	1%

Radii measurements are taken from the Empire State Building as a reference point.

The perpetrator is a foreign terrorist group and the terrorist attack falls within the definition of an 'Act of Terrorism' as set out in TRIA.

Non-TRIA Event

The same scenario as above, but the perpetrator is a domestic terrorist group and the event is not covered by TRIA.

PRESCRIBED ASSUMPTIONS

Number of Deaths and Injuries

1,000 blue/white-collar worker deaths in total and 2,500 injuries in total: syndicates to determine a worst case split across lines of business (WCA, PA, Group PA, etc.) and document assumptions using the commentary facility in the RDS Reporting Software. The following percentage split should be used for non-fatal injuries:

- 14% life threatening
- 35% moderate
- 51% minor

Finanzgruppe
Deutscher Sparkassen- und Giroverband

How to Set Up And Successfully Operate a Data Pool

The First Reason Why You May Wish to Participate in a Data Pool

Stupid men do not learn from their mistakes.

Smart men learn from their mistakes.

Wise men learn from others‘ mistakes.

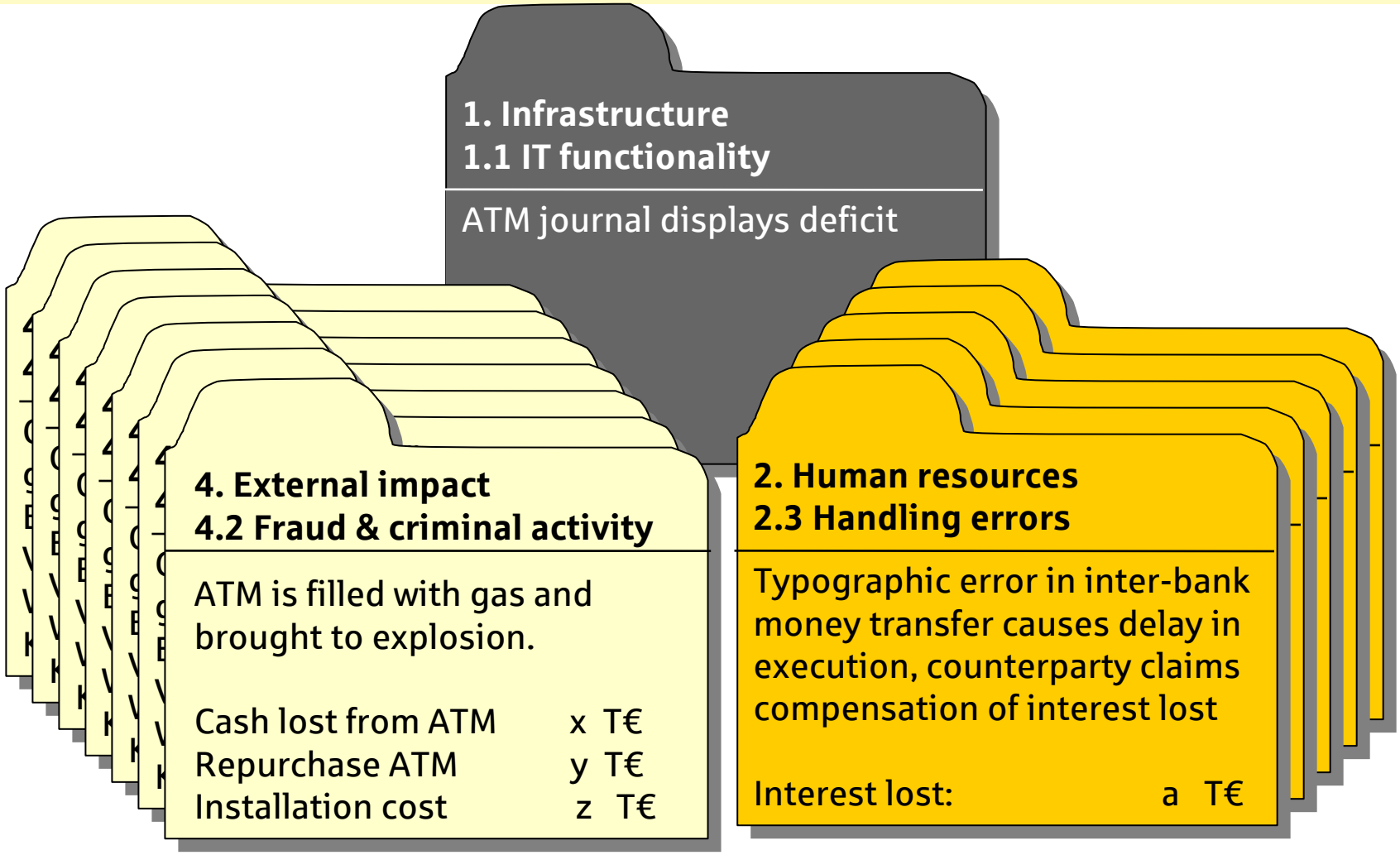
A Good Data Pool Can Serve Many Purposes

- Provide scaled information on losses to participating institutions
  - Complete, anonymized categorization, description, valuation of loss scenario, action taken (if applicable)
  - Our pool: 31 items / loss
- Provide scaling model and scaling factors
- Support peer group formation to facilitate exchange of practices and benchmarking
- Provide a data base sufficient to allow quantification of operational risk (e.g. bank with balance sheet of 3 bln. € has 25 losses > 1000 € per year)

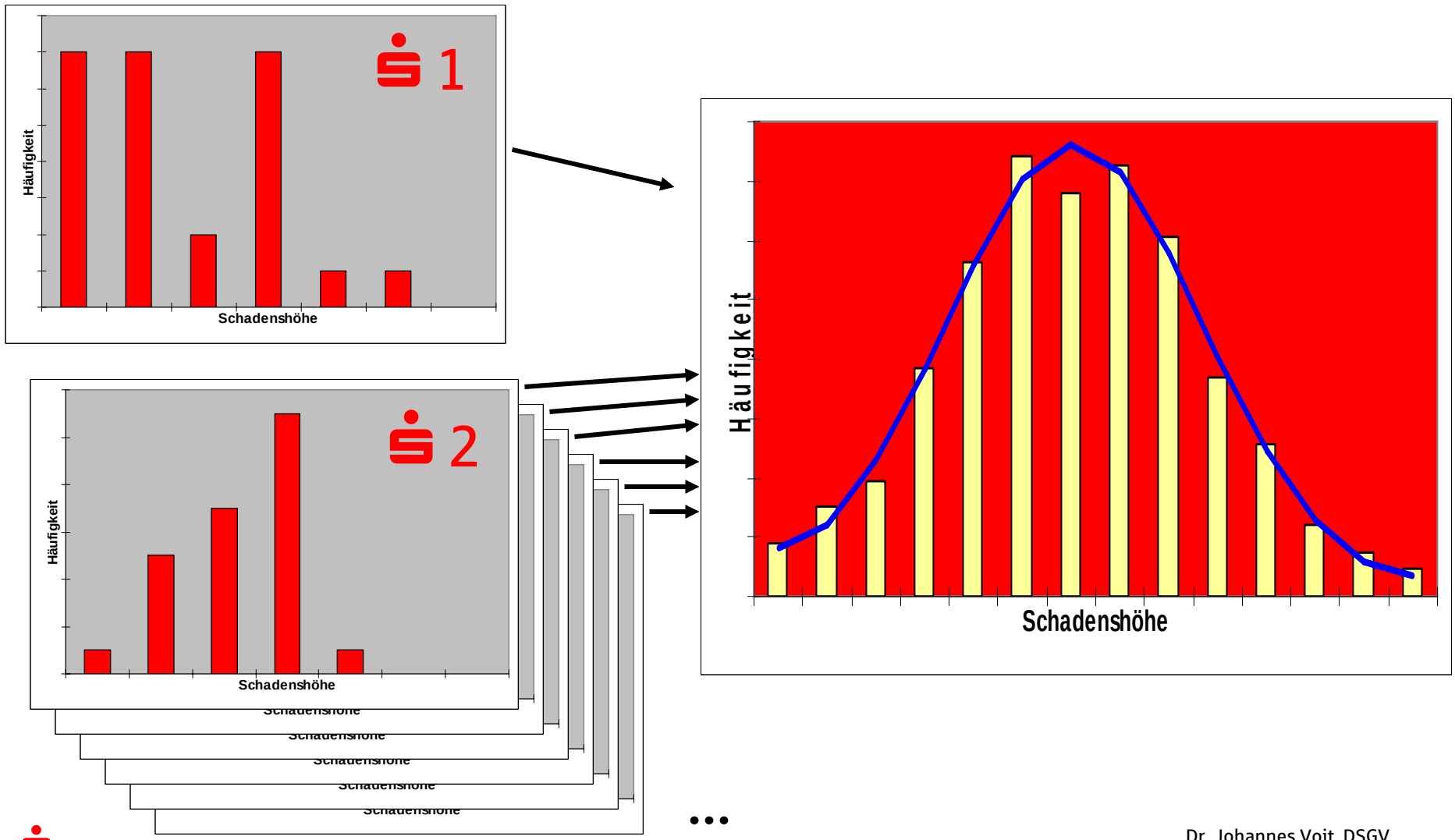
The Loss Data Pool Is Heavily Used – in Particular by Small Institutions

Number of savings banks	85 i.e. 113 bank years
Balance sheet of participating banks	200 mln. € ... 30 bln. €, median ≤ 2 bln. €
Number of losses	3,756 i.e. average 33 per bank and year
Total loss amount	33.3 mln. € gross, 13.1 mln. € net
Average loss	8,900 € gross, 3,500 € net
Median loss	1,900 € gross, 1,000 € net
Number of losses ≥ 10,000 € gross	355
Number of losses ≥ 100,000 € gross	41

From the Start, Almost 4,000 Losses Have Been Contributed And Can Be Analyzed



The Second Reason Why You May Wish to Participate in a Data Pool



Finanzgruppe
Deutscher Sparkassen- und Giroverband

Scenarios and Pool Data: Are They a Cornerstone Or Afterthought in Calculating OpRisk Capital

Scenarios and Pool Data Are a Cornerstone of Our Capital Calculation

	Var (99,9%)		Var (99,9%)
L. Infrastructure	0	Sc. Infrastructure	1,795,000
L. Human Resources	468,000	Sc. Human Resources	4,622,000
L. Internal Processes	0	Sc. Internal Processes	2,499,000
L. External Impact	118,000	Sc. External Impact	4,370,000
Internal losses	**472,000**	**Scenarios**	**7,872,000**
Dp. Infrastructure	1,997,000	Infrastructure	1,891,000
Dp. Human Resources	1,476,000	Human Resources	2,532,000
Dp. Internal Processes	1,937,000	Internal Processes	1,941,000
Dp. External Impact	529,000	External Impact	3,338,000
Data pool (rescaled)	**2,919,000**	**Bank (aggregated)**	**6,760,000**

- Technically: credibility theory
- Our data histories are short, scenarios and pool data essential.

Scenarios And Pool Data Can Also Be Used As an Afterthought to Capital Calculation

- Capital calculation based on loss data alone („normal case“) – when sufficient data available
- Scenario analysis and pool data then for stress test resp. ICAAP
- Consider stress scenarios (“extreme, but still plausible”), and the biggest external losses available, and calculate capital requirements (realistic disaster scenarios for banks)
- In general, when $CAP_{stress} > CAP_{normal}$
  - Capital supplement, i.e. $CAP \geq CAP_{stress}$
  - Action plan to make sure that capital is sufficient. But in OpRisk, does one have time to act when the scenario materializes?
- Stress testing in CEBS CP 12 – but no mention of operational risk there. Focus on market, credit, liquidity.

Finanzgruppe
Deutscher Sparkassen- und Giroverband

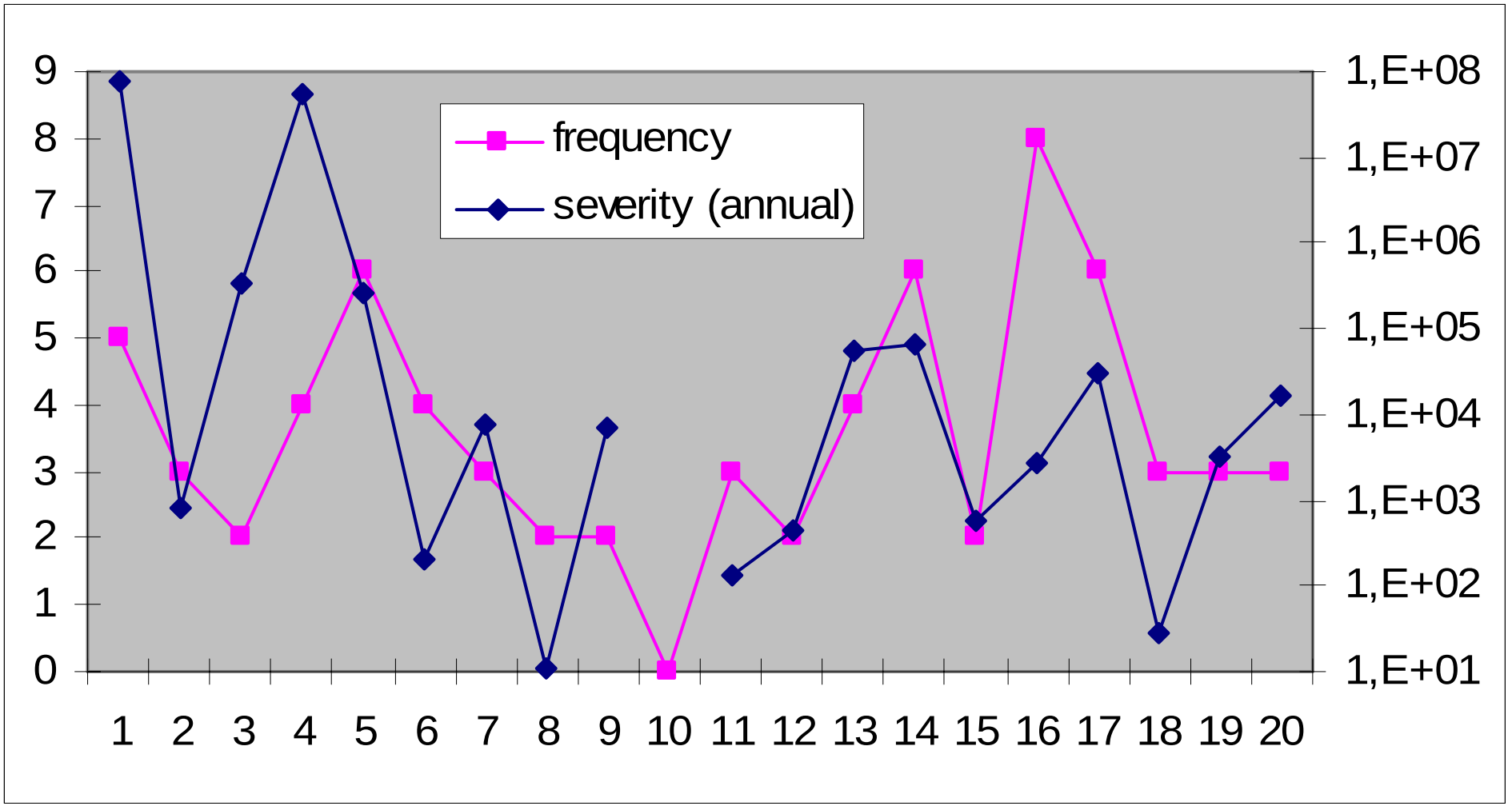
Using Scenarios And Pool Data to Drive Process Improvements

What Happens to Operational Risk Management When It Is Based on Internal Loss Data Alone?

- Frequency is a random variable, average possibly not converged (law of large numbers)
- Severity is a random variable, average possibly not well converged, but also not meaningful. Quantiles of severity distributions even less well converged.
- Random arrival times of internal loss events: random action
- No priorities set.
- Not forward looking

- Except for very-high-frequency events leveraging loss data is a necessity for driving process improvements (and management action generally)

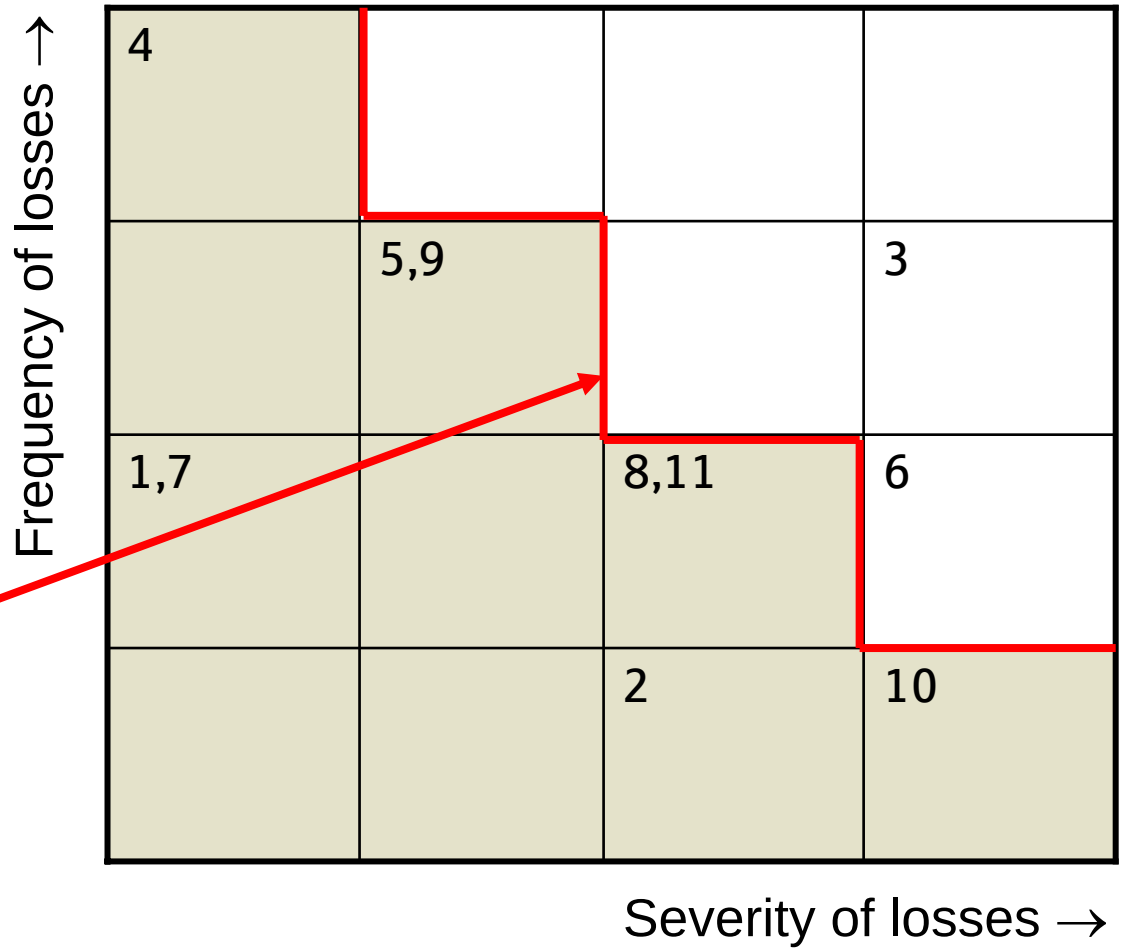
Loss Events Are Random Numbers (Standard Model of Actuarial Science)



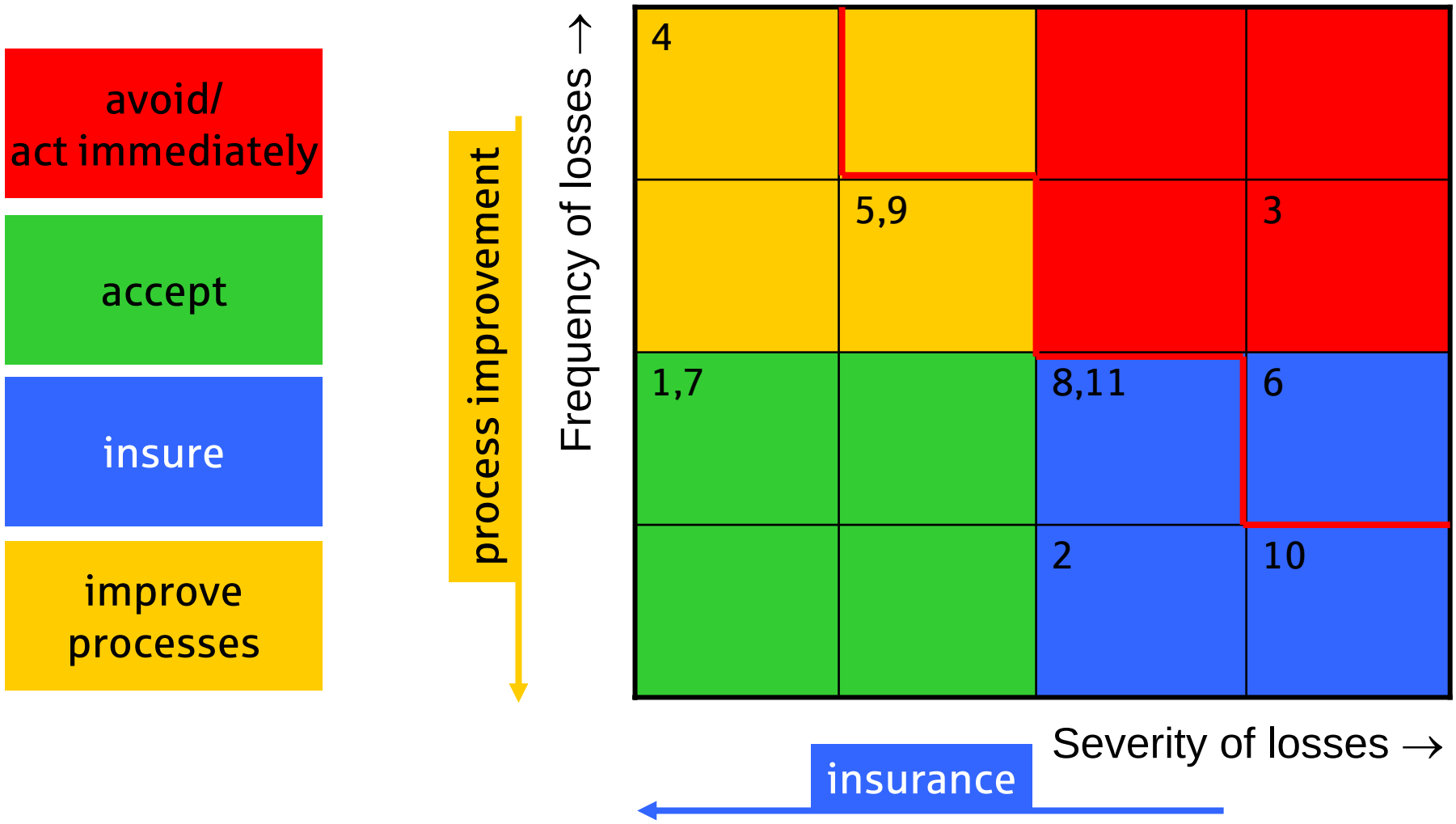
The Bank Is a Portfolio of Businesses – And of Operational Risks

1...11:
Business lines,
Activities, ...

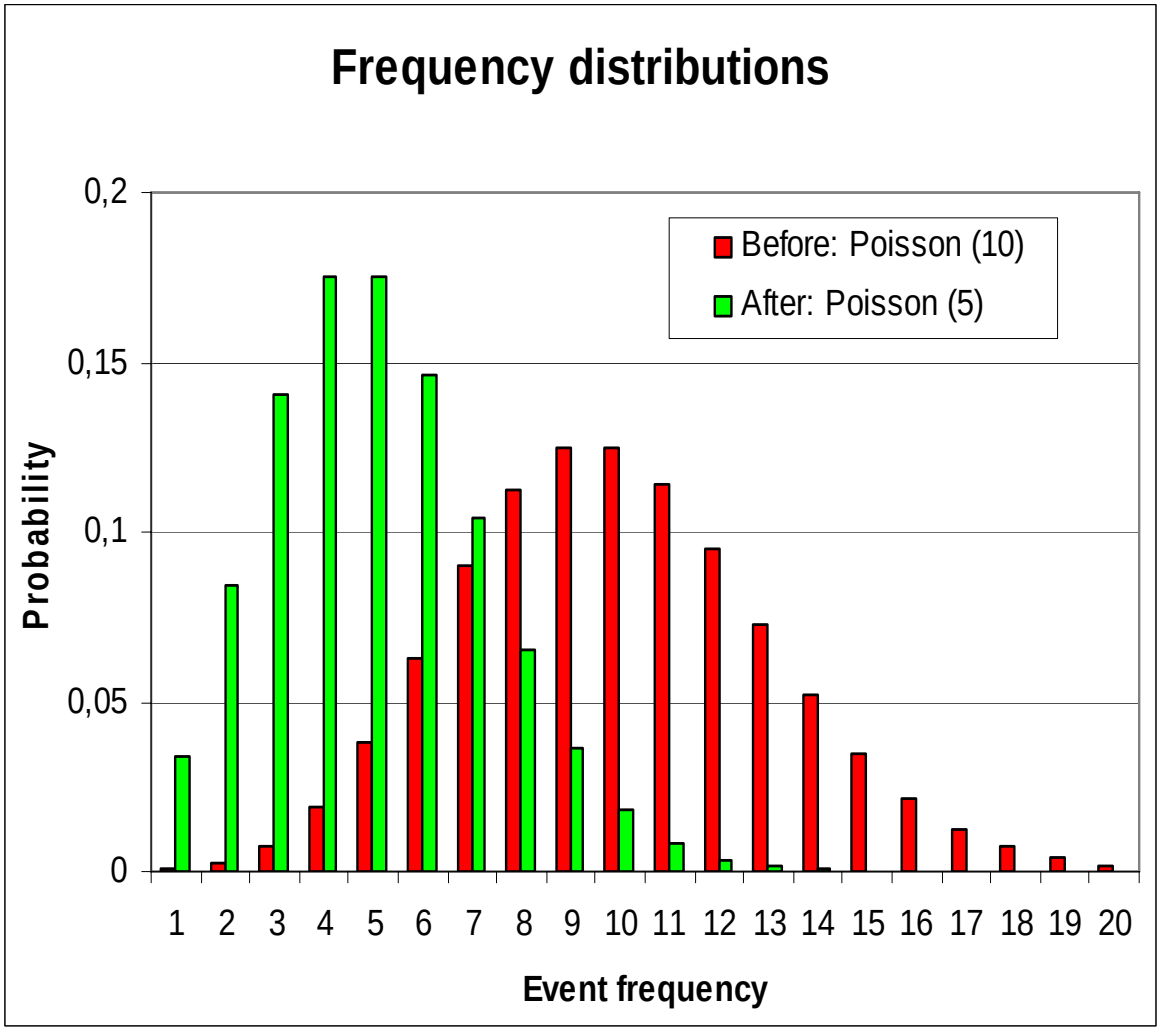
Risk tolerance
Risk appetite



Management Action Depends on Frequency and Severity of Losses



When Scenario Analysis Is a Cornerstone, We Can Use It to Ex-Ante Evaluate Management Action



Severity distribution: How does it change?

Consequence for expected losses and capital?

<u>Investment decision:</u>
Cost of implementation and maintenance smaller than savings on expected losses and cost of capital?

Speaker‘s Details

Dr. Johannes Voit
Deutscher Sparkassen- und Giroverband
Charlottenstrasse 47
D-10117 Berlin (Germany)

Phone: +49 30 202 25 5412
Email: johannes.voit@dsgv.de