Using Scenario Analysis to estimate Operational Risk Capital

David Palmer
Director
Credit Suisse First Boston

OpRisk Europe 2005
17 March 2005

CREDIT SUISSE | FIRST BOSTON

Overview

- The nature of Operational Risk
- Practical implementation challenges
- The irrelevance of small losses to capital
- Correlation assumptions
- Implementing a scenario-based capital estimation approach
- Benchmarking OpRisk capital estimates
- Conclusion

The nature of Operational Risk

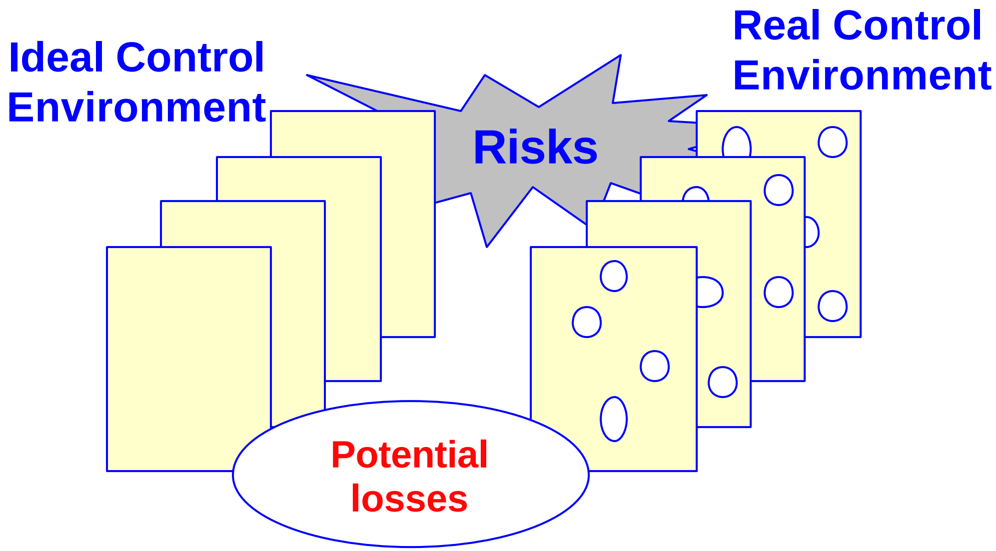
A1. Types of OpRisk

Goal of OpRisk management is to reduce the frequency & severity of large, rare events

	Small Losses	Large Losses
Low Frequency	**Doesn't matter much**	**"MAJOR" events** **(Primary challenge)** • Can put banks (e.g. Barings) out of business or severely harm reputation • Difficult to understand and prioritize in advance • Similar to issues faced in several other industries: aviation, healthcare, railways, chemical processing
High Frequency	**"MINOR" events** **(Secondary challenge)** • Generally not firm threatening • Experience makes it easier to understand problems, to measure issues & to take relevant action • Can often be incorporated into pricing - "cost of doing business" (e.g. credit card fraud losses) • Generally generates efficiency savings rather than reduce material risks	**Not Relevant** (Otherwise would already be out of business!)

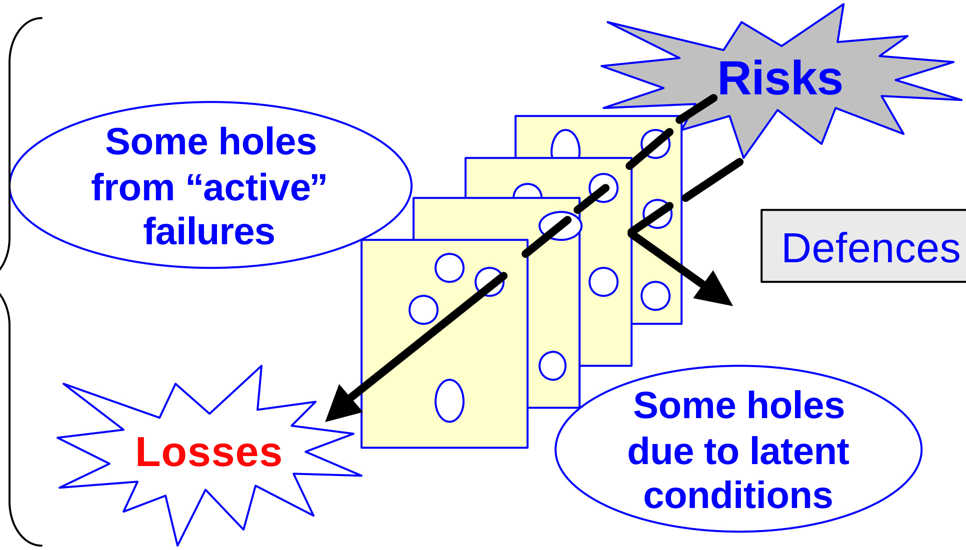
A2. “Swiss cheese” model – “Major” OpRisk events

- **“Swiss cheese” analogy – holes exist in all systems**
- **Risk of accidents can be mitigated by developing effective “defenses-in-depth”**
  - Successive layers of protection each designed to protect against the possible breakdown of the one in front
- **Defensive control layers try to minimize occurrence of large organizational accidents**



“Major” OpRisk events more unlikely as they require alignment of holes in successive control layers

e.g. bad person; flawed systems; poor management; weak controls, on a bad day . . .



Source: “Swiss cheese” model (Adapted from Reason, 1997)

A3. Applying the "Swiss cheese" model

Ideally defensive controls would be sufficiently tight so risk can be eliminated.

In reality gaps and weaknesses are inevitable, especially in fast changing environment

(1) Focus on multiple layers of defense

- Avoid simplistic preoccupation with a single defense - beware of the human desire for a simple flaw or scapegoat
- Improving any one of the layers can meaningfully reduce the risk or loss
- Spend time working on fixing/ reducing holes in each layer - Group actions into families of strategies that correspond to management hierarchies so that there can be ownership of improvements

(2) Don't over-focus on Active Failures - address underlying Latent Conditions

- **Latent conditions: arise from strategic and other top-level decisions – the impact spreads throughout the organization creating error-producing factors within the workplace**
  - Examples: inadequate systems, poor supervision, inadequate training, poor design, lack of risk ownership, dysfunctional compensation schemes, lack of ownership culture
  - May be present for many years before they combine with other failures to breach the defenses
- **If latent conditions remain unchanged then efforts to improve things at the workplace/level will be limited - certain kinds of error just replaced by new types of error**
  - Requires thoughtful defense design and long term view

(3) Regularly reassess and update for changing environment

- Defensive control layers and associated "holes" are not fixed and static - in reality, they are constantly moving, e.g. headcount changes, new/changing business/markets, control breakdowns
- Other holes created through intentional violation of rules/policies/procedures, e.g. Bad people will learn about gaps in defenses

A4. Strategies/principles to reduce proneness to accidents

There are a number of strategies/principles that have been used in other industries that are most promising for reducing the likelihood of adverse events:

(1) <u>Rationalization/stratification</u>: Reducing the entropy or complexity of systems

- Reduce number of systems to appropriate number while maintaining flexibility to support business
- Many solutions to fewer; Avoid one size fits all, eg. replace with 5 sizes fits 90%

(2) <u>Simplification/standardization</u>: Reducing the complexity of processes

- Simplify processes – reducing number of steps, number of hand-offs
  - E.g. if single step has 99% success rate then 10-step process has 0.99x0.99x…..x0.99 (10 times) = approx. 90% success rate
- Standardize across like processes

(3) <u>Use constraints & forcing functions</u>: Constraints restrict certain actions – Forcing functions ensure certain actions performed

- Constraints: use of limits; choosing from number of provided choices; inputs ranges/validation
- Forcing functions: to ensure data entered; ensure correct following of sequence

(4) <u>Make doing the right thing easiest</u>: Design processes/systems so that the safe/controlled action is the one that requires least effort

- E.g. use default choice for most frequent action

(5) <u>Respect limits on vigilance and attention</u>: Design for normal human behaviour

- Keep in mind issues of workload, stress, limits of memory, attention; Use checklists

Practical implementation challenges

B1. Comparing OpRisk with market risk and credit risk

The table below compares OpRisk with market and credit risk, considering each characteristic in turn and its impact on the ability to quantify OpRisk.
While market and credit risk have many similarities, OpRisk is very different.

		Market Risk	Credit Risk	Operational Risk
Risk position	Quantifiable exposure	Yes	Yes	Difficult*
	Exposure measure	Position; Risk sensitivity	Money lent; Potential exposure	Difficult – no ready position equivalent available*
Completeness	Portfolio completeness	Known	Known	Unknown
Context dependency & data relevance	Context dependency	Low	Medium	High
	Data frequency	High	Medium	Low*
Measurement & validation	Risk assessment	VAR; Stress testing	Rating & loss models	No true risk models
	Accuracy	Good	Reasonable	Unproven
	Testing	Adequate data for backtesting	Backtesting difficult to perform over short term	Results very difficult to test over any time horizon
	Summary	Market risk models well established and proven tools	Using models considered reasonable – but should be used with care	Models yet to be proven

* Unlikely other than for certain high-frequency low-loss events, e.g. settlement losses.

B2. What are the features of a good risk model?

- **Mathematical models are used in market and credit risk management for decision making purposes because they provide the user with information on the potential losses that can be incurred for a given portfolio of positions**
  - There is a clear linkage between the generators of risk (interest rate dv01s, equity price sensitivities and money lent) and the potential financial impact on the firm
  - Linkages can subsequently be tested and provided to work
- **What should qualify as a "risk model" - A model is a mathematical representation of a real-life situation which should be realistic enough to provide good a understanding of the main elements of the situation in question. Features of good models include:**

  (1) they capture the essential features of the situation in a plausible manner (i.e. <u>there is a direct and measurable linkage between risk drivers and the level of risk</u>)

  (2) they <u>have predictive qualities</u> that can be used for decision making purposes

  (3) those <u>predictions agree with known facts and can be validated</u>
- **At a minimum, a good risk model should enable you to judge whether Bank A is riskier that Bank B, and whether Bank A's risk is increasing or decreasing over time**
  - Market and credit risk models generally satisfy these requirements
- **OpRisk "models" also need to demonstrate these features**

B3. The 4 elements of the AMA

- **A bank's AMA OpRisk model must include the following 4 elements:**
  - (1) Internal loss data
  - (2) External loss data
  - (3) Scenario analysis
  - (4) Business environment & internal control factors
- **There are a number of practical implementation issues with each of these 4 elements:**
  - Completeness; Accuracy; Auditability; Relevance

	Completeness	Accuracy	Auditability	Relevance
Internal loss data	LOW/MEDIUM (1)	HIGH	HIGH	LOW (2)
External loss data	LOW (3)	LOW (3)	LOW/MEDIUM (3)	MEDIUM
Scenario analysis	MEDIUM/HIGH	MEDIUM	LOW/MEDIUM	HIGH
Business environment & internal control factors	LOW	LOW/MEDIUM(4)	LOW/HIGH (4)	HIGH

Conclusion

The elements that are easy to audit aren't very relevant

The elements that are most relevant are harder to audit

Notes

(1) More difficult to ensure completeness for high-frequency, small-loss events "Minor" events; easier for "Major" events

(2) Low rating as most firms unlikely to have suffered numerous "Major" events to provide sufficient data sample

(3) Low/medium rating due to reporting bias and collection bias

(4) Medium accuracy and auditability for factors that are countable but Low otherwise

B4. OpRisk capital approaches considered

The industry has divided into 2 main approaches for determining OpRisk capital:

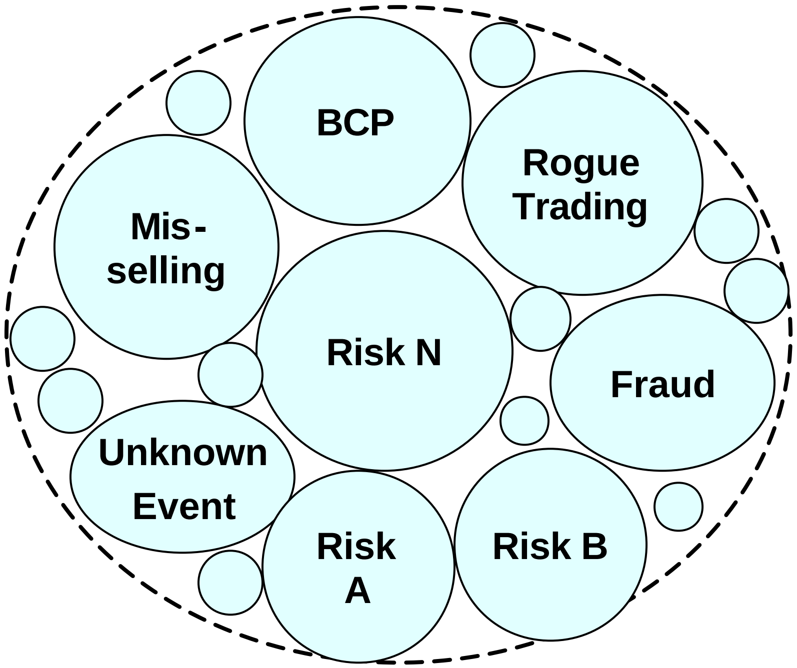
- **<u>Loss data modeling</u> approach has limitations, since it is so reliant on data**
  - Approach based on collecting actual internal and external oprisk losses that have occurred
  - Frequency and severity distributions are then estimated from collected data
  - Numerous practical issues with availability and relevance of data collected:
    - Firms change over time reducing the relevance of the data collected
    - Management actions are taken to prevent future reoccurrence of internal events
  - Results are also very dependent on the distribution assumptions used
- **<u>Scenario-based approach</u> chosen as most appropriate approach to determining an OpRisk capital figure for the high-impact low-frequency events that drive the AMA capital estimation**
  - Utilises relevant internal and external loss data, business environment and internal control factors and other relevant data, such as knowledge of the future plans of the firm (forward looking)
  - Uses such data in an objective way, using expert judgement to determine its relevance
  - Top-down scenario analysis approach ensures that all material risks are identified
  - Pragmatic approach that gives reasonable top line result; Cost effective to implement
  - Easier to adapt and adjust to changing circumstances
  - Transparent process that provides a useful OpRisk management process in developing scenarios

In practice, many banks use a hybrid of the above two approaches

B5. Scenario analysis

- **To address the issue of completeness of the portfolio of OpRisk exposures one needs to determine a set of exposures (and their associated probabilities of occurring)**
  - Primary focus is on the "major" events, e.g. rogue trader, building unavailability, etc.
  - Secondary events may also be included to improve completeness
- **The aim is to fill the OpRisk "Event Space" as fully as possible with all possible major scenarios**

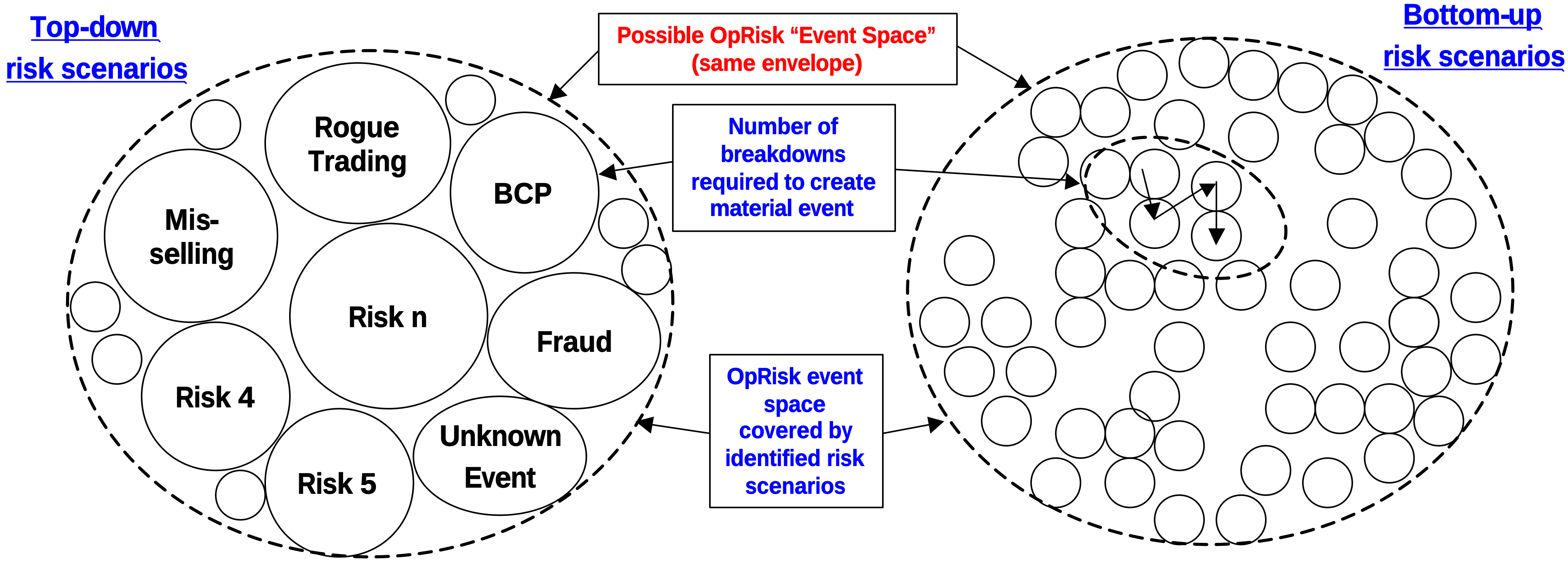
OpRisk "Event Space"



- **Important to note that many of the biggest OpRisk losses arise from fundamentally new issues & hence difficult to foresee**
  - There will be some element of the Event Space not covered by a known risk – unknown risks – but with top-down approach we can include an "Unknown Event" scenario

B6. Scenario analysis: Top-down vs bottom-up

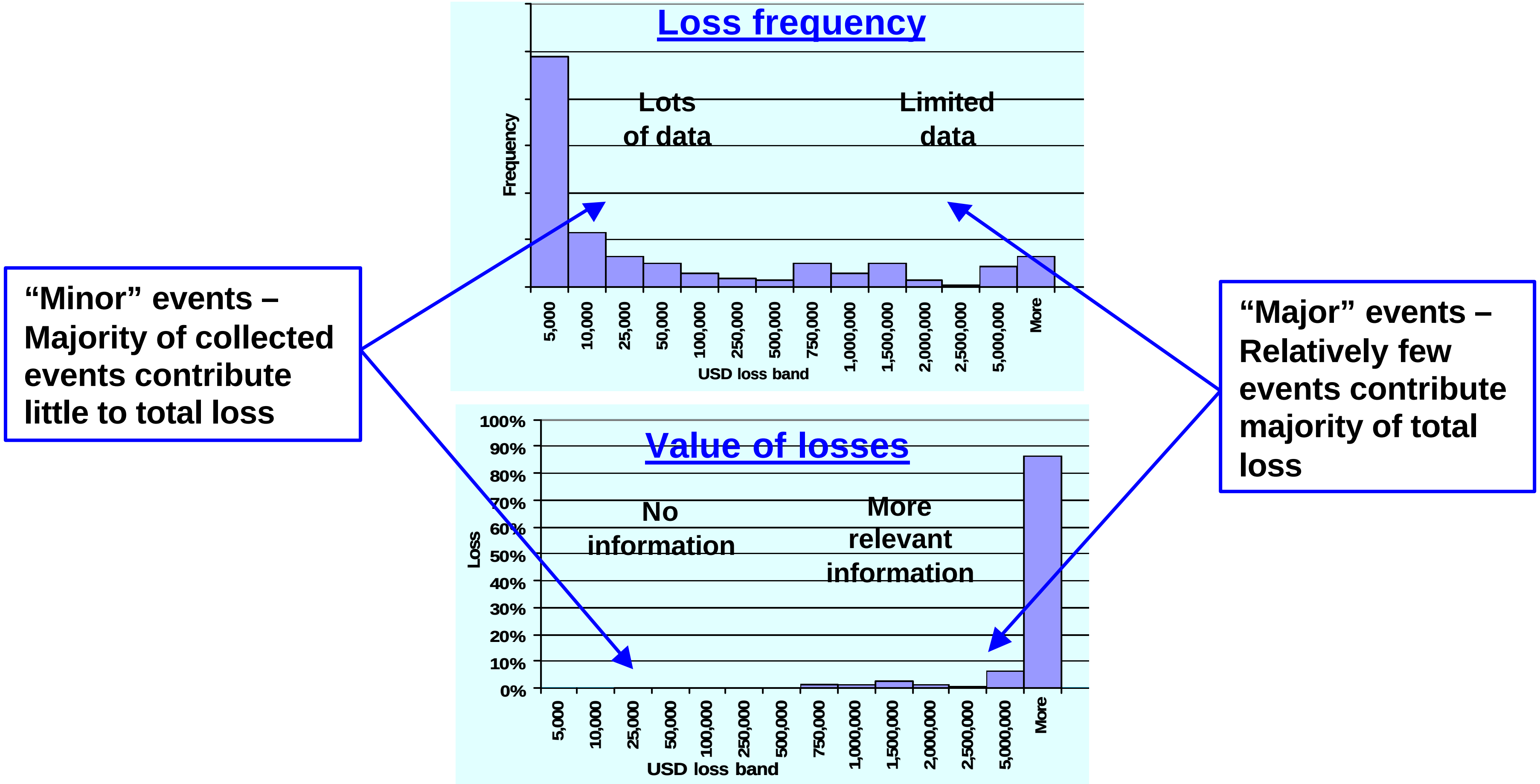
- **The OpRisk event space can be equally covered through top-down or bottom-up risk identification**
  - With top-down risk identification, many low level risks and control failures can be encapsulated within a single scenario
  - With bottom-up risk identification, risks are more numerous but more micro in scope
- **Top-down scenario analysis approach ensures that all material risks are identified**



The irrelevance of small losses to capital

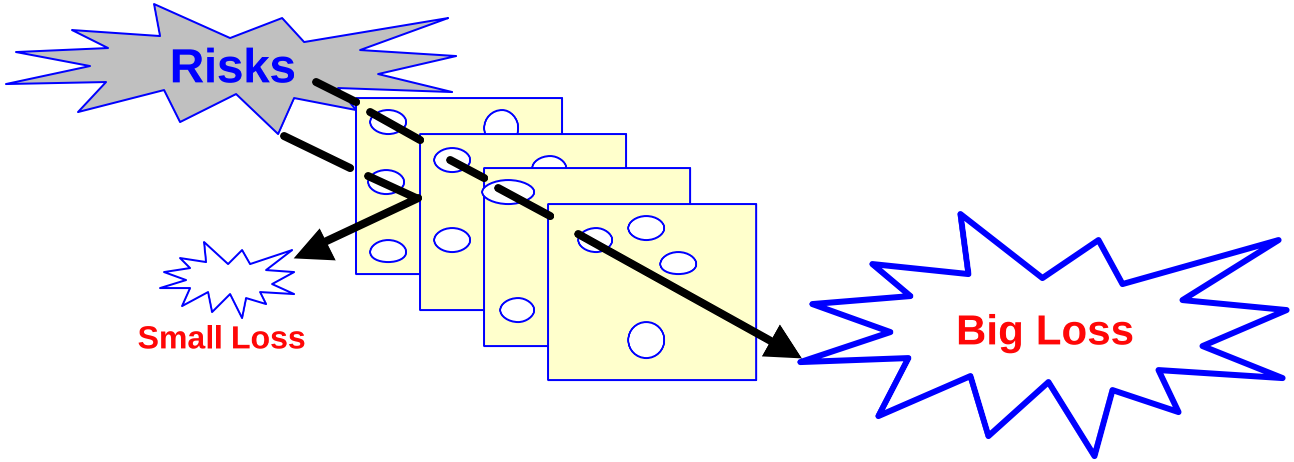
C1. Experience/observations of loss data collation

- It is important to understand why internal loss data is being collected. How is the data going to be used? Must not confuse "data" with "information"



Conclusion: All relevant information is obtained from "Major" OpRisk loss events

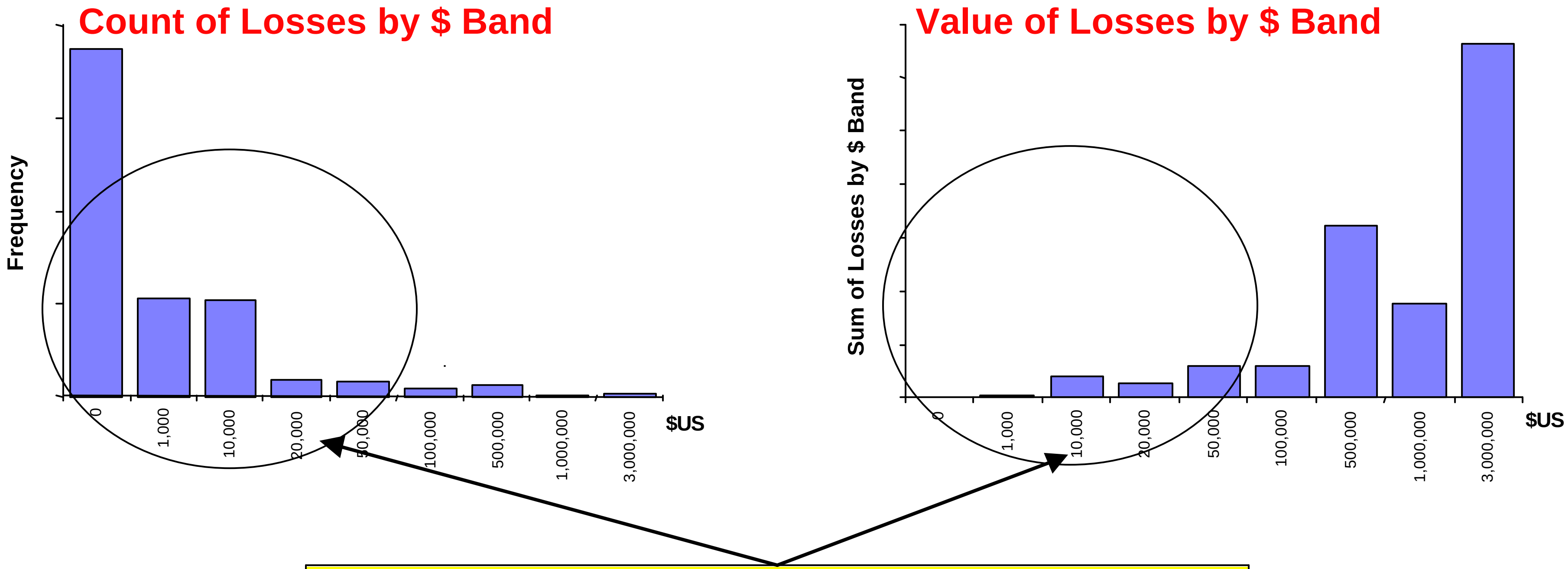
C2. Nature of small OpRisk losses vs large OpRisk losses



	Small Losses	Large Losses
How caused?	▪ Small number of control layers breached ▪ Generally control failure is specific to a particular department	▪ Typically many control layers breached ▪ Control failures cross a number of departments
Typical examples	▪ Settlement errors	▪ Fraud; rogue trader; business interruption
Appropriate Actions	▪ Lessons learned only relevant to processes within the particular dept concerned ▪ Often actions taken only require reinforcement of minor changes to controls already in place ▪ Escalation only relevant to dept management	▪ Lessons learned often read across multiple departments ▪ Often require new controls or significant re-design of existing controls ▪ Escalation required across departments
Appropriate loss reporting	▪ Department escalation and reporting processes sufficient	▪ Central aggregation and reporting required

C3. Analysis of Operations OpRisk losses - (1) by loss band

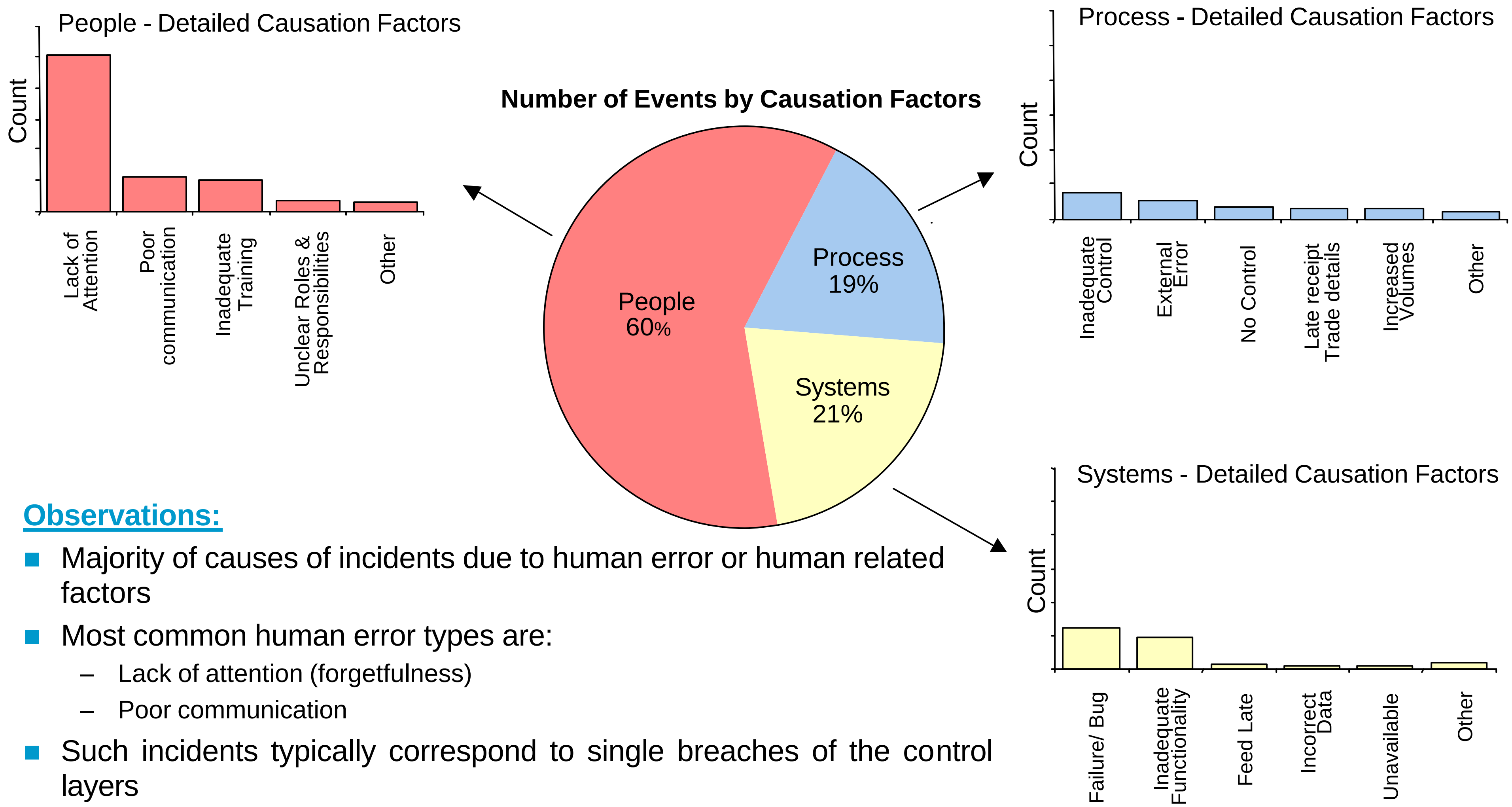
- **To investigate the nature of small OpRisk losses, the losses of the Global Operations department were analysed**
- **A similar pattern to that for the whole firm can be seen:**



Observations:
- Majority of losses constitute relatively little to total loss
- Under $50k events contribute only 10% of the total loss value
- 5% of the losses account for more than 90% of the total loss

Source: Global Operations department

C4. Analysis of Operations OpRisk losses - (2) by cause



Observations:

- Majority of causes of incidents due to human error or human related factors
- Most common human error types are:
  - Lack of attention (forgetfulness)
  - Poor communication
- Such incidents typically correspond to single breaches of the control layers
  - Shows that the successive defense layers provide adequate control to capture upstream control breaches

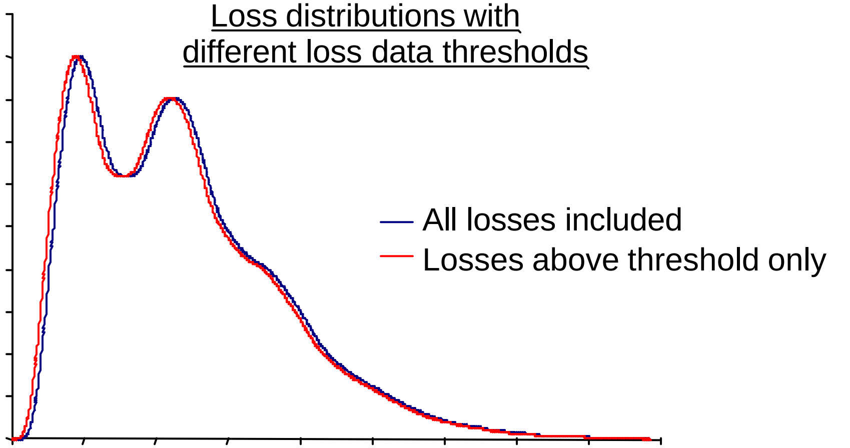
Source: Global Operations department

C5. Irrelevance of small OpRisk losses to OpRisk Capital

- **Experience indicates that the majority of cumulative loss derives from a small number of large events –minor OpRisk event losses provide limited relevant information**
- **Therefore, only material losses significantly impact the level of capital**
  - Small losses are expected – they are "the cost of doing business"
  - Impact of small losses is immaterial in relation to levels of capital held by bank, therefore almost irrelevant to the capital calculation

Tasche's Rule

- **Tasche's formula provides an accurate estimate of the level of capital required to cover the small losses if they are excluded from the loss population used in determining the capital charge**
- **The quantile of a combined population of large and small losses is estimated as the quantile of the large losses plus the expected value of the population of small losses**

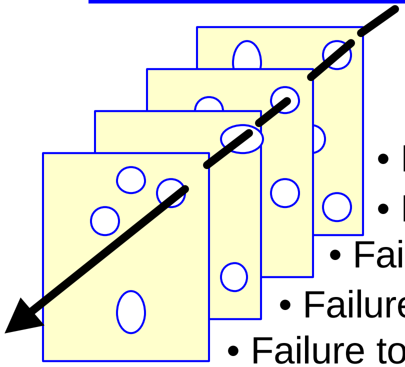


Correlation assumptions

D1. Correlation assumptions

- **Correlations are considered at 2 levels: (1) within a scenario, (2) across scenarios**
- **Correlation within scenarios: 100% correlation between individual control failures**
  - e.g. "Major" rogue trader event is the combination of: lack of supervision **&** failure to obtain confirmations **&** failure to independent test prices **&** failure to perform independent P&L analysis **&** …
- **Correlation across scenarios: 0% correlation between major event scenarios**
  - No evidence to suggest that OpRisk events are correlated, e.g. what is the likelihood of documentation failure impacting building unavailability

"Major" event – eg. Rogue Trading

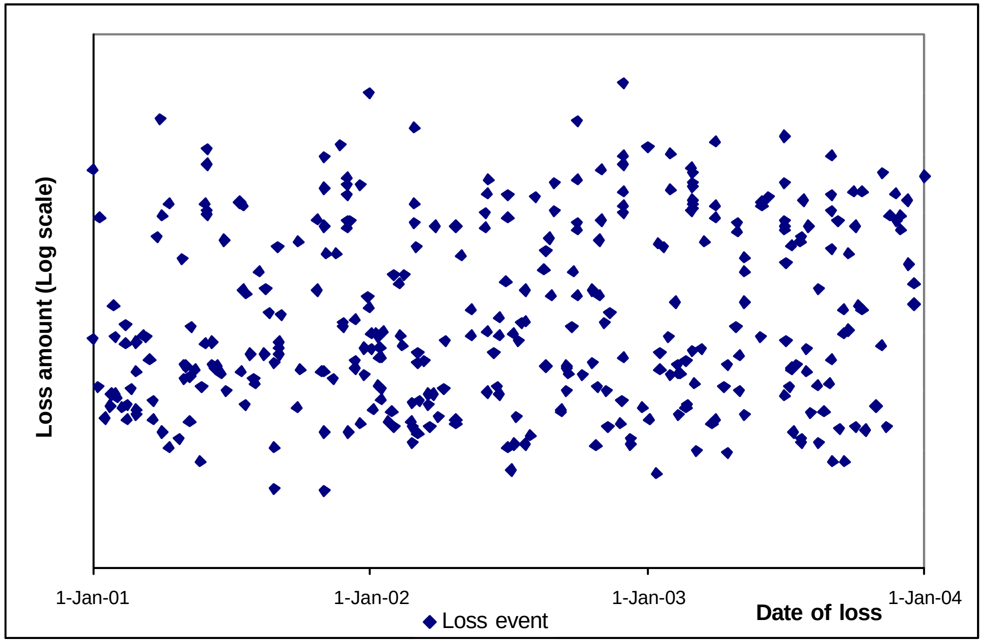


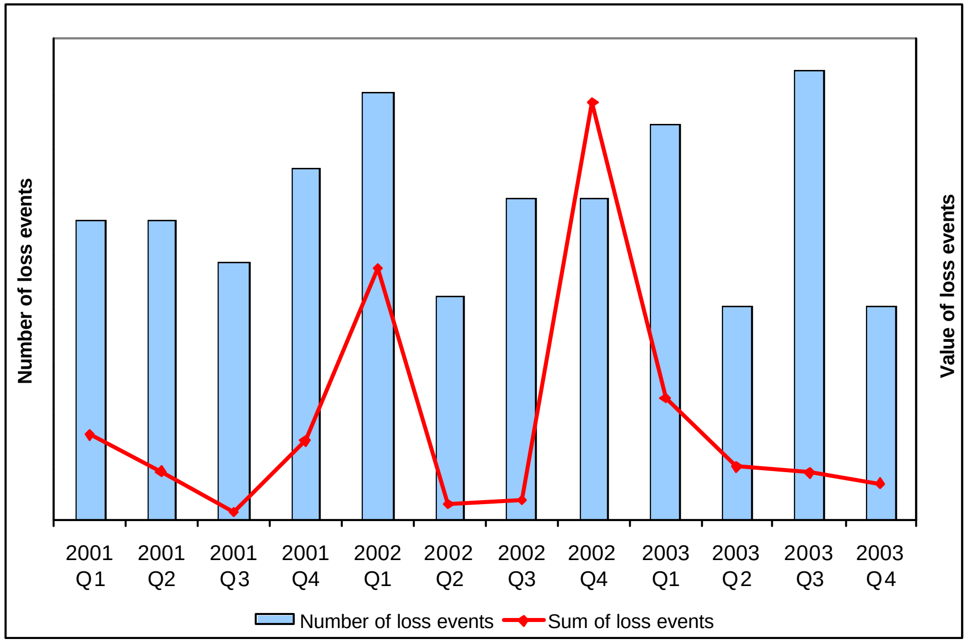
- Lack of supervision
- Poor challenge, issue escalation
- Failure to obtain transaction confirmations
- Failure to obtain independent FX prices
- Failure to analyse P&L

"Major" event is the combination of individual control failures that alone would not give rise to the incident (i.e. 100% correlation between individual control failing)

D2. OpRisk aggregation: Across scenarios

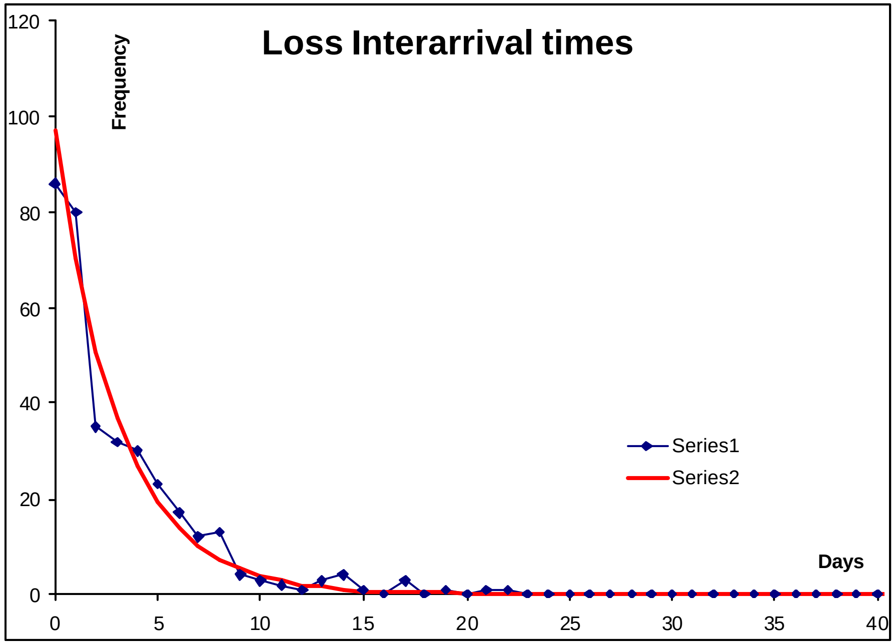
- **Scatter graph of severity of loss event vs date of arrival shows no pattern**
  - Indicates no relationship between one event and another
- **There is no strong relationship between the number of loss events and the aggregate value of loss events**
  - No obvious relationship between number of losses and aggregate value of losses is evident – suggests that the level of OpRisk is not related to the number of events suffered

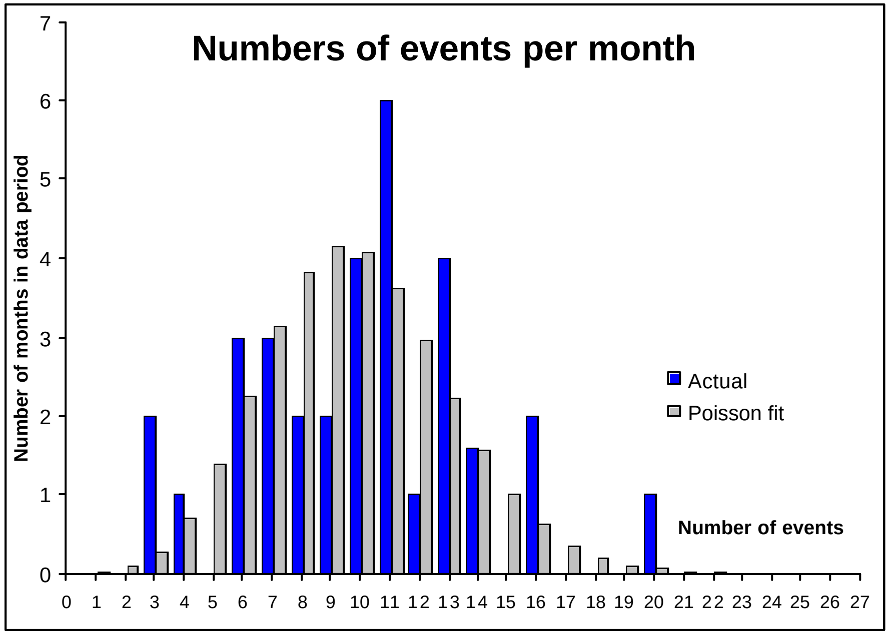




D3. OpRisk aggregation: Across scenarios

- **Loss interarrival times & correlation: Actual loss experience**
  - From OpRisk loss data it is possible to estimate the distribution of <u>interarrival</u> times, i.e. the days elapsing between each loss event and the next event in sequence
  - <u>For independent events, interarrival times should be approximately exponentially distributed</u>. Fitting an exponential distribution allows the average interarrival time to be estimated





<u>Conclusion</u>

- **Evidence confirms common-sense, i.e. intuitive that OpRisk events are not correlated**
- **OpRisk scenarios should be aggregated with 0% correlation**

Implementing a scenario-based capital estimation approach

E1. OpRisk capital process overview – 3 stage process

1. OpRisk scenario identification → Determine scenario parameters
2. Business experts review → Scenario template updates
3. Senior mgt committee review → Finalise OpRisk capital figures

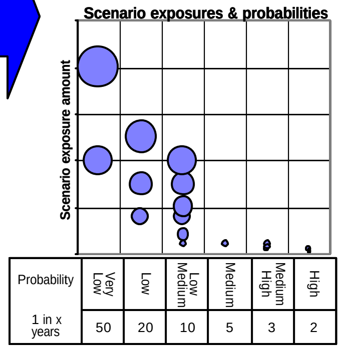
- **Calculating OpRisk capital is a 3 stage process:**
  - (1) Identify OpRisk scenarios and parameters
  - (2) Review by business experts
  - (3) Senior management committee review and approval

Internal loss data

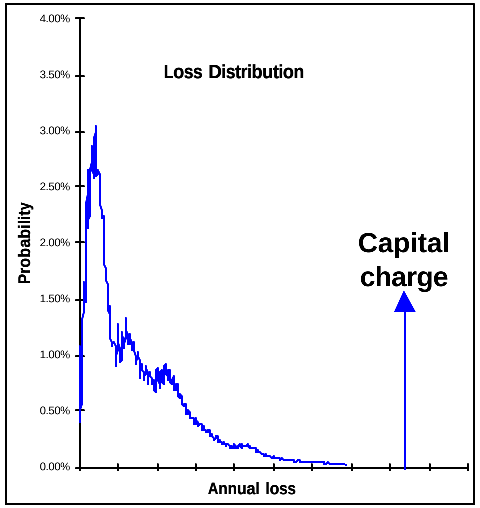
External loss data

Business environment & internal control factors

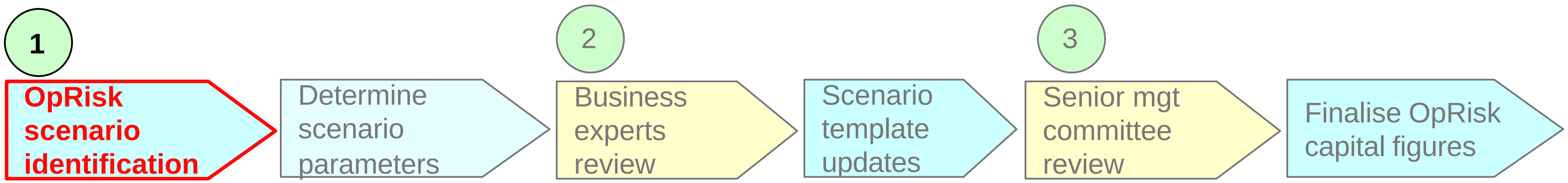
Scenario definitions & parameters



Aggregation of scenarios using OPRISK+



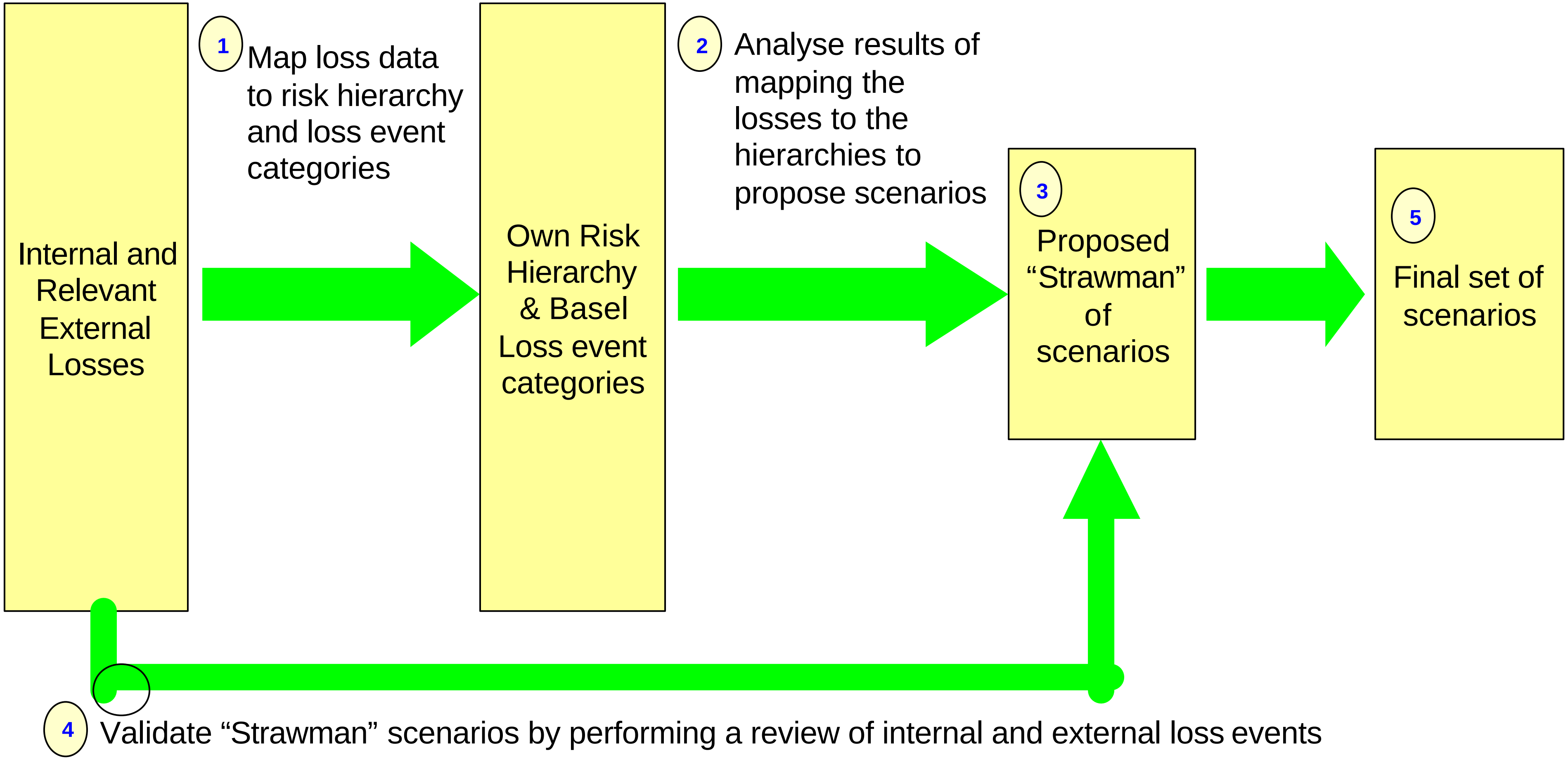
Stage 1a - Determining the set of OpRisk scenarios



E2. Determining the full set of OpRisk scenarios (1)

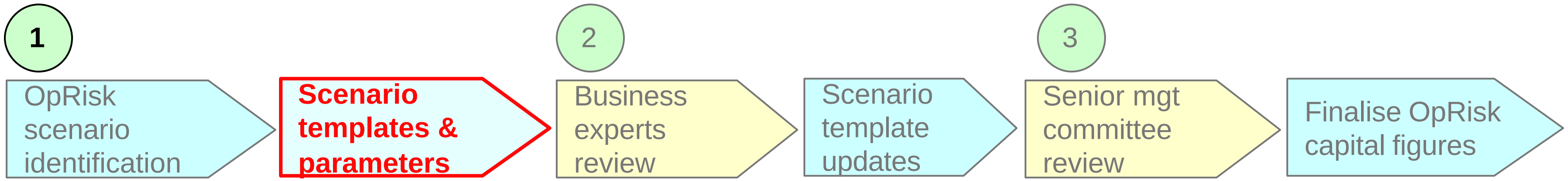
- **Internal and external loss data is mapped to existing risk hierarchies to provide a framework for analysis**
  - Mapping to Basel loss event categories and to own risk hierarchy
  - To allow focus on material risks, losses are aggregated to identify concentrations (e.g. aggregate by number and sum of losses against each risk type)
- **“Strawman” set of scenarios is proposed**
  - Based on the analysis of concentration of losses from the above step and expert judgment
- **Validate “strawman” scenarios through review of external and internal loss events**
  - Map the external and internal loss events to the proposed scenarios to ensure that they are all covered
  - Minimise overlap between proposed scenario definitions to limit the loss events that map to more than one scenario – i.e. ensure scenarios are independent
  - Make any scenario changes or amendments to the scope and coverage of the definitions to ensure that all loss events are covered by a scenario
- **Refine scenario risk coverage throughout discussion with business experts**
  - When discussing scenarios with business experts ensure all known risks are covered
- **<u>Target is for the scenario set to cover 100% of the OpRisks of the firm</u>**

E3. Determining the full set of OpRisk scenarios (2)

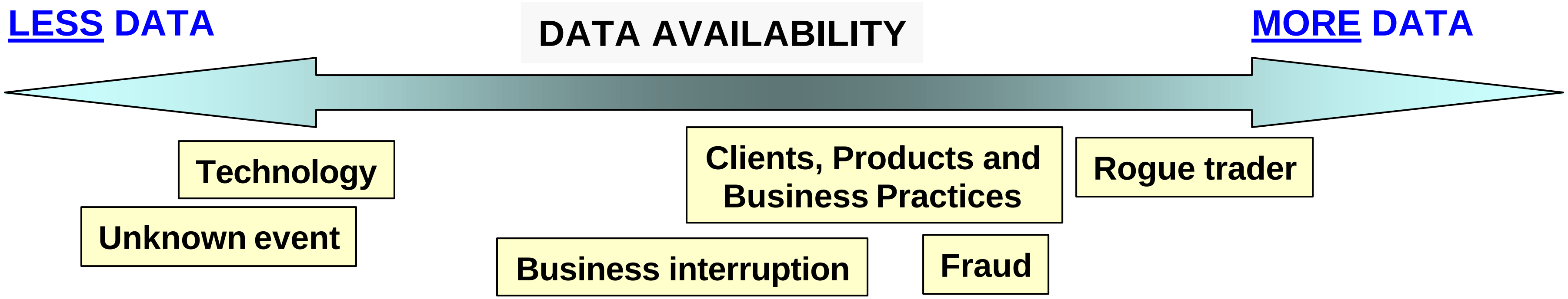


The target is for the scenario set to cover 100% of the OpRisks of the firm

Stage 1b - Determining the scenario parameters



E4. Limitations of internal and external loss data



There are a number of challenges of using internal and external loss data:

- **<u>Data availability/relevance</u>:** Limited relevant internal or external loss data will necessarily mean that scenario severity and frequency parameters are subjective
  - More data: e.g. rogue trader events (esp. large events) typically get publicly reported
  - Less data: e.g. limited data currently available for technology losses
- **<u>Limited predictive value</u>:** Internal and external loss data are not necessarily good predictors of future events – after a "major" event, actions taken by management would improve controls that would reduce likelihood of future re-occurrence
- **There are numerous reporting/data capture issues with external loss data – data needs to be used with care**
  - <u>Reporting bias</u>: Relies on companies disclosing significant OpRisk loss events and on OpRisk loss events being reported correctly in publicly available documents
  - <u>Capture bias</u>: Relies on firms capturing accurately OpRisk loss events and amounts from publicly available documents

E5. Use of internal loss data

- **The uses of internal loss data <u>are limited</u> when using a scenario approach to estimate OpRisk capital**
- **Internal loss data is more useful in considering the types of adverse loss events that could occur:**
  - The loss amount provides only a single data point
  - More useful to consider the potential range of losses that could occur from the event type
- **Actual internal loss data is used in the parameter determination process as a guide to potential severities and frequencies of loss events that have occurred**
  - Consideration is given to the frequency of historical loss events and the typical magnitude
  - Generally it is more useful for determining the risk of lower-severity scenarios, rather than the really large-severity events (since it is unlikely that the firm will have experienced many of these)
  - Internal data is also more useful for determining the risk of lower-severity scenarios since reporting bias will limit the amount of external loss data available
- **Internal loss data is sometimes thought to be more relevant to the firm than external data – but context dependency and actions taken after an event means this relevancy is short-lived**
  - In a well-controlled bank the amount of internal loss data points that are relevant/material from a capital viewpoint should be limited
  - Management and regulators will expect banks to change/update internal controls after an event

E6. Use of external loss data

- **External loss data is the <u>most useful data source</u> in considering the key types of adverse loss events that could occur and their likely magnitude**
  - Unlikely that a firm will have suffered many high-severity events itself, so internal data will be limited
  - External data allows the firm to use the experiences of other firms to make sensible estimates of scenario parameters
- **However, data is still context dependent and relevancy needs to be assessed**
  - After a material external loss event at one firm, all firms will make a review, assess their own controls, and implement appropriate control changes reducing the relevancy even further
- **A peer group of banks can be defined that are similar to the firm:**
  - Based on products traded, locations and markets covered, etc.
  - These can be given extra priority when assessing the magnitude of scenario parameters
  - Data events are generated from a known population of firms, allowing scenario frequencies to be <u>estimated</u> as number of events divided by peer institution years:
    - Number of institution years estimated from number of peer institutions and the number of years over which the external data is likely to be reasonably reliable
    - However, this is not an exact science and expert judgement is still required
- **Can also use “thought experiments” for certain scenarios:**
  - E.g. “How often would you expect to see a major news story re: rogue trader loss >$500m affecting your peer group?”
  - This analysis is most appropriate for the scenarios with a significant amount of external data for review: Rogue Trading; Clients, Products and Business Practices; Fraud

E7. Business environment & internal control factors

- **There are a number of potential dimensions of business environment and internal control factors (BE&ICFs), including:**
  - Complexity: Business/product, technology, business processes, organization, legal entity
  - Rate of change of markets/products/volume: Developing vs. matured
  - Management: Centralised vs. remote; own managed vs. outsourced
  - Processing maturity: Automatic straight-through-processing vs. manual
  - Personnel: Level of turnover; level of resourcing; competency of resourcing
- **Although possible to justify each business environment and internal control factor as a driver of risk, it is generally only possible from a directional basis rather than absolute**
  - Greater benefit is obtained from using business environment and control factor indicators (e.g. KRIs) to track change in individual risk factors than attempting to convert into aggregate economic value
- **Some elements are auditable at the specific factor level but are difficult to translate or "dollarize" into an economic amount – even harder to aggregate across factors**
  - E.g. what is the economic value of one outstanding confirmation acceptance vs. one depot break?
- **Incorporating BE&ICFs into the assessment of scenario severity and frequency parameters is a complex subjective process that can only be made by experienced experts**

E8. Example: Rogue trader scenario – loss data

- **Internal loss data:**
  - There is limited internal loss data
- **External loss data:**
  - Data analysis suggests that the size of the loss is related to the length of time over which the rogue trading activity occurred (i.e. time to discovery) => 3 sub-scenarios of differing magnitude created relating to differing time to discovery

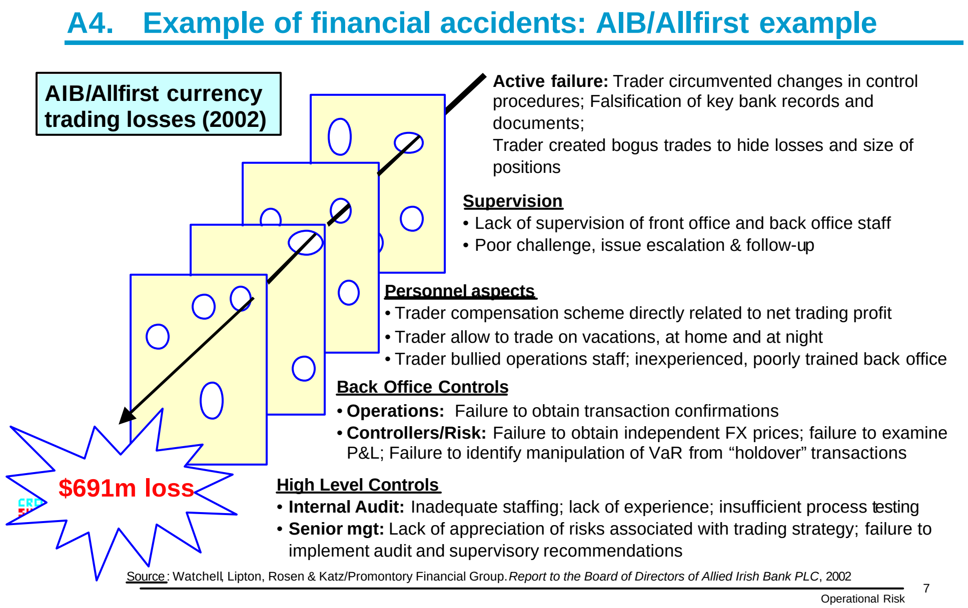
Comparison of peer events vs. parameters used for capital estimation

	No. of losses	Losses/Institution Year
Number of loss events >$500m	**1**	**0.01**
Number of loss events >$100m and <$500m	**2**	**0.02**
Number of loss events >$10m and <$100m	**3**	**0.03**

- **Observations:**
  - Frequency of 1 in 100 years appears reasonable for a large rogue trader loss (>$500m)
  - Losses between $100m and $500m are also rare from the peer group data with 2 events in 100 institution years
    - The scenario frequency is probably more prevalent than the peer data suggests (reporting bias)
  - Loss events under $100m start to contain completeness issues in the external data
    - Internal data can be used to assist in determining the parameters for this scenario

E9. Example: Rogue trader scenario – BE&ICFs

- **Rogue trading losses typically occur due to the failure of multiple control layers (slices of cheese) – e.g. AIB/Allfirst**
  - Incorporating BE&ICFs is a complex and subjective process for rogue trading risk
  - Hence a mechanistic incorporation of BE&ICFs could lead to inappropriate management incentives



- **Examples of BE&ICFs that could be considered for rogue trading:**
  - Supervisory training (enhanced supervision of traders reduces the risk of unauthorised activity)
  - Systems enhancements/weaknesses (strategic systems vs. spreadsheets; improved booking controls; increased straight-through-processing)
  - Trade surveillance

E10. Example: Technology scenario

- **Internal loss data:**
  - Limited internal loss data relating to technology risk
  - Hence not possible to perform any analysis using internal data to determine severity and frequencies
- **External loss data:**
  - There is also limited external loss data relating to technology risk
  - Hence not possible to perform any analysis using external data to determine severity and frequencies
  - External news events highlight the risks associated with technology (e.g. viruses) which are factored into the scenario considerations
- **Business environment & internal control factors:**
  - Examples of BE&ICFs for technology risk include:
    - Business Continuity Planning: reduces the severity in the event of an IT failure
    - Software Development Lifecycle: reduce the risk of inappropriate or flawed releases of software
  - Consideration also given to how changes to the environment associated with Technology affects the risk of this scenario – e.g. continuing increased prevalence of wide-scale virus attacks
- **Observations:**
  - The lack of internal and external data does not mean that the technology risks faced are low, but just that the industry has not yet suffered a significant financial loss due to these risks
  - Due to the lack of internal/external data, the analysis has to be subjective, based on expert judgment

E11. Calculating the OpRisk capital & incorporating insurance

Overview of mathematics required

- **<u>The model mathematics are simple</u>**
  - Once you have determined the set of scenario probabilities and severities, a variety of different methods can be used to calculate the overall capital charge
  - No curve fitting and minimal quantitative support is required
  - The model is stable in the tails of the distribution
- **The OpRisk capital can be calculated using a simple mathematical event risk model**
  - Methods that could be used to calculate the capital charge include: binomial tree methodology, Monte Carlo techniques, actuarial models (e.g. Panjer's algorithm) or simple convolution techniques
  - You can even use your credit risk model; just change the inputs into the model: substitute OpRisk scenario severities for credit exposures and OpRisk scenario probabilities for the credit default probabilities
  - Model converts the scenario parameters into an aggregate loss distribution from which the required capital quantile can be identified

Incorporating insurance

- **Insurance is easily incorporated into the framework by adjusting the severity parameters to be net of insurance mitigation**
  - Map insurance policy coverage against scenario risks
  - Calculate likely insurance recovery based on scenario loss event, taking into account policy limit, deductible and an appropriate haircut, and reduce scenario severity accordingly

Stages 2&3 – Expert review and documentation

1. OpRisk scenario identification → Scenario templates & parameters →
2. **Business experts review** → **Scenario template updates** →
3. **Senior mgt committee review** → **Finalise OpRisk capital figures**

E12. Scenario templates and expert review

- **Draft up scenario templates using a standardised format:**
  - Description of scenario risk
  - Description of primary controls mitigating the risk
  - Summary of internal and relevant external loss experience related to the scenario
  - Description of any relevant BE&ICFs affecting scenario risk or control environment
  - Other relevant information – e.g. insurance cover
  - Assumptions used to determine parameter assumptions
  - Summary of scenario parameters (frequency and severity)
- **<u>Scenario templates provide the key documentation to evidence how the scenario parameters have been determined</u>**
  - Essential for review by internal and external auditors and very useful for regulatory reviews
- **Review each scenario template with business experts**
  - Utilises the full range of skills and experience in the firm; invite all relevant experts who may have something to say about a particular scenario
  - Discuss scenario risk, controls and scenario parameters with the relevant experts, utilizing their expert judgment (e.g. discuss the Fraud scenario with experts from Legal, Corporate Security and Operations)
  - Update scenario templates to reflect feedback from experts
- **Final stage is review of capital assessments with Senior Management**
  - Provides an additional sense check over capital numbers

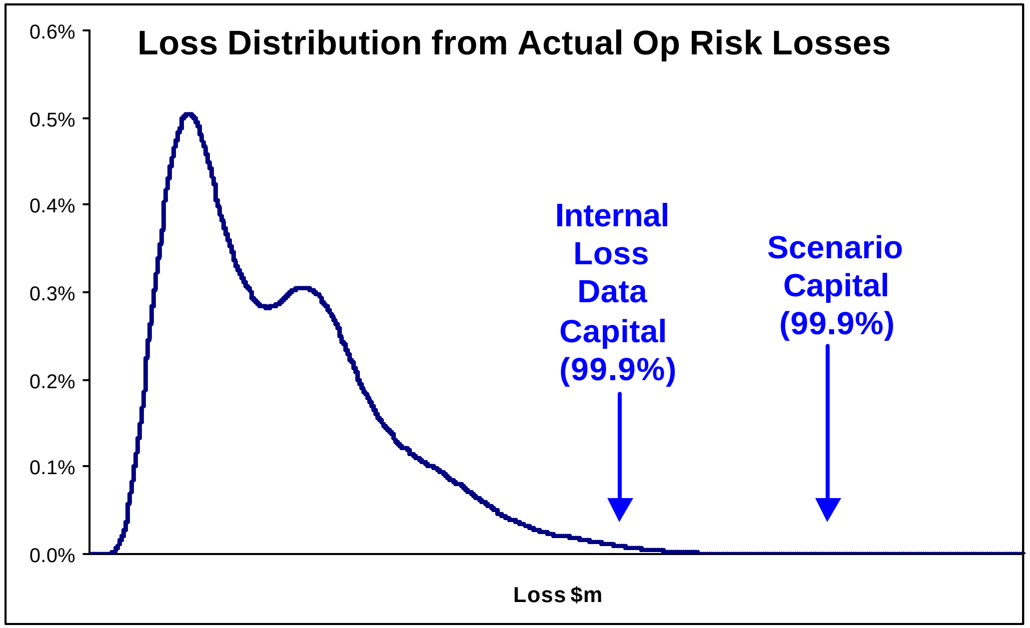
Benchmarking OpRisk capital estimates

F1. Benchmarking: Against internal loss data

- **"Validation" of OpRisk models is a major challenge – pure statistical validation of OpRisk models may not be possible for many years, <u>probably never</u>**
  - The fundamental challenge for any OpRisk model is that the system changes in character before adequate data is accumulated to validate the model (esp. for low-frequency, high-impact events)
- **However there are benchmark tests that can be performed for scenario approaches:**

Against <u>Internal</u> OpRisk Loss Data

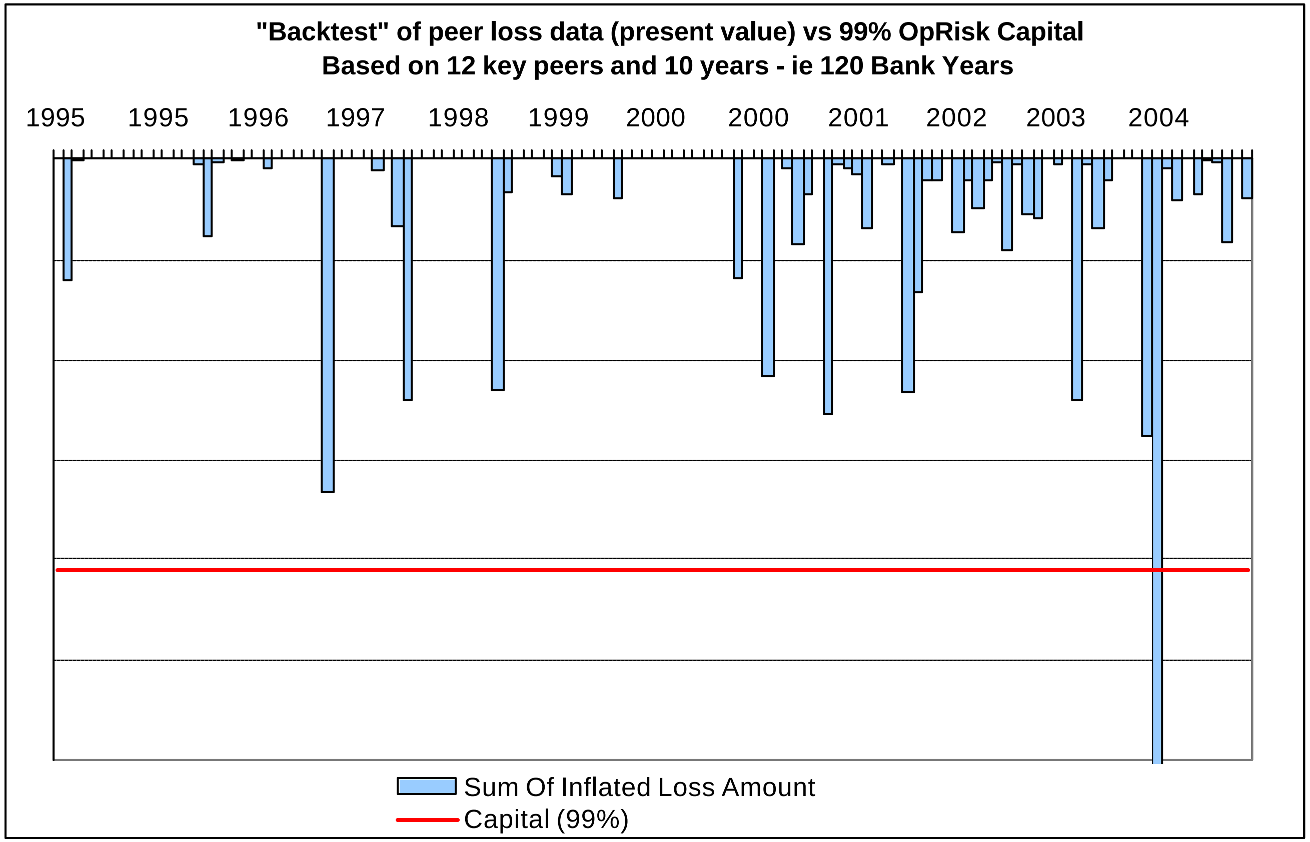
- **Graphs show loss distribution from actual internal OpRisk loss data over 3 yr period**
  - No assumptions are made regarding the underlying distribution of events



F2. Benchmarking: Against external loss data

Against <u>External</u> OpRisk Loss Data

- **Graph shows aggregated annual OpRisk loss amounts for 12 key peers over 10 years (i.e. 120 institution years of relevant data)**
- **99%-ile OpRisk figure (red line) is equivalent to 1 in 100 year event**



Conclusion

G1. Conclusion

Characteristics of Scenario Approach

- **A scenario-based capital estimation approach is: pragmatic; implementable; cost effective**
- **Sensible capital numbers can be derived in a systematic and transparent manner**
- **The mathematics required is simple and stable in the tails of the distribution**
- **Expert judgment is used to blend all types of available data with understanding of the control environment to produce forward-looking assessments of risk**
- **The process to determine the scenario parameters is a useful management process in its own right, ensuring discussion amongst experts and senior management of the key risks the firm faces**

Have a go yourself……

- **Re-perform the analysis in this presentation on your own data**
- **What does your loss data tell you?**
  - Frequency plot; value vs. number of losses plot; cumulative loss ranking; scatter plot vs. time; interarrival times; etc.