

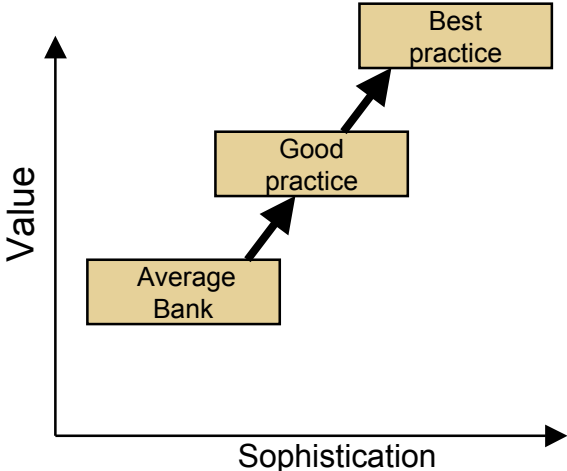
The Implementation of an Operational Risk Management Framework

Dr. Christian Terp

Geneva, 7th December 2000

- **Introduction**
- **Qualitative Assessment**
- **Quantitative Assessment**
- **Organizational Aspects of Operational Risk Management**
- **Lessons Learned**

Need for Operational Risk Management

Need for Operational Risk Management	Changing Environment	New Industry Practices
<p>Internal Factors:</p> <ul style="list-style-type: none"> • Lack of transparency for the management • Lack of awareness, definitions and culture • Dependence on technology • Increased product complexity • Increased transaction volume • Shortage of qualified staff and staff turnover <p>External Factors:</p> <ul style="list-style-type: none"> • Spectacular operational loss cases: Barings, etc. • Protection of reputation • Legal: KonTraG 	<ul style="list-style-type: none"> • Globalization /functional structure • Competitive Environment & cost allocation • Regulation (e.g. BIS) • Business diversity <ul style="list-style-type: none"> • increasing product complexity • restructuring to address market need 	 <p>Best Practice:</p> <ul style="list-style-type: none"> • Consistent framework • Organizational structure in place • Ongoing risk assessments • Link to capital allocation • Integrated risk management (market, credit, operational risk) • OR awareness part of corporate risk culture

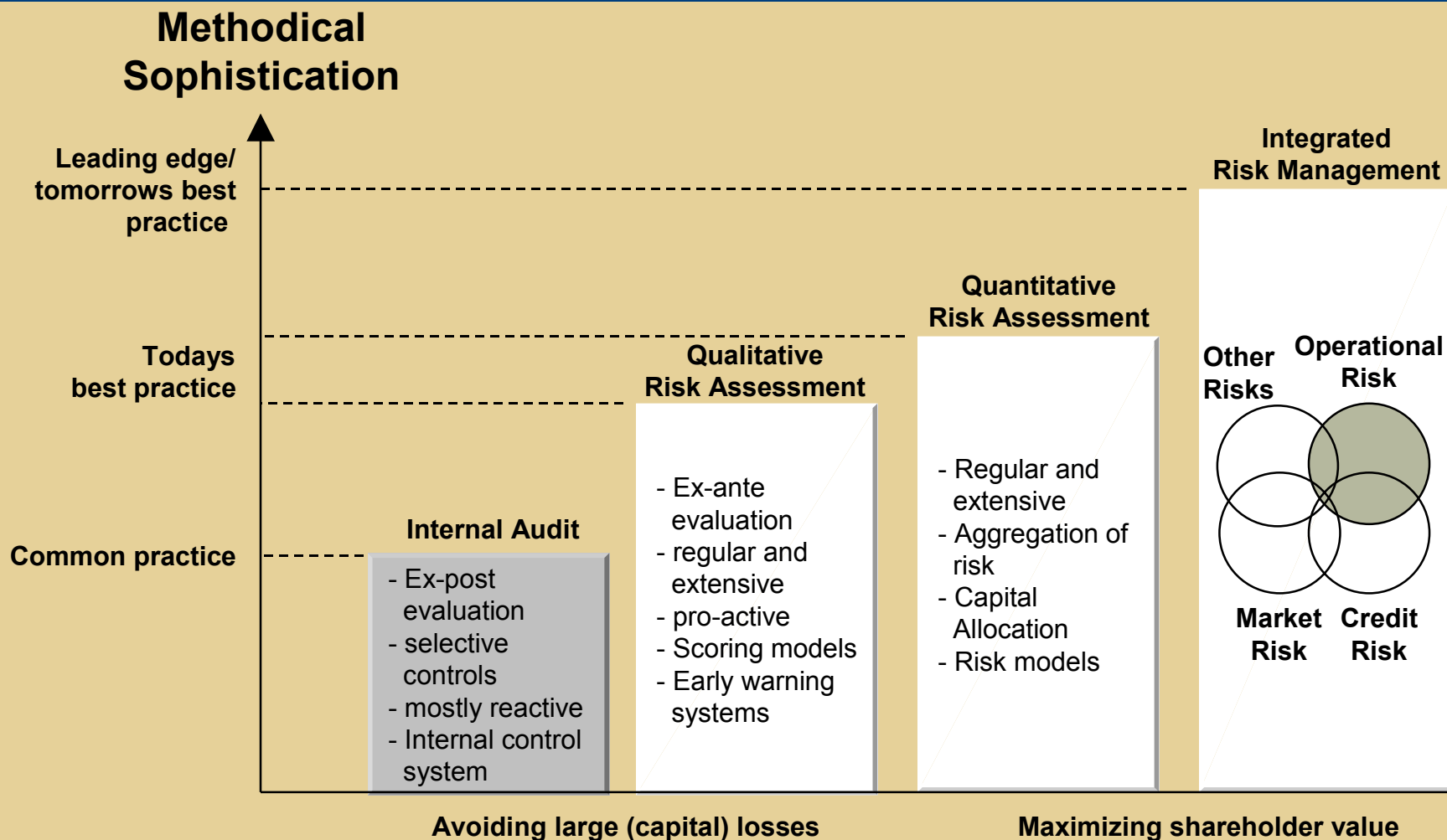
Current situation for many banks:

- Fragmented approach (responsibilities, ...)
- No (consistent) methodology
- No integration with market and credit risks

Benefits of Operational Risk Management

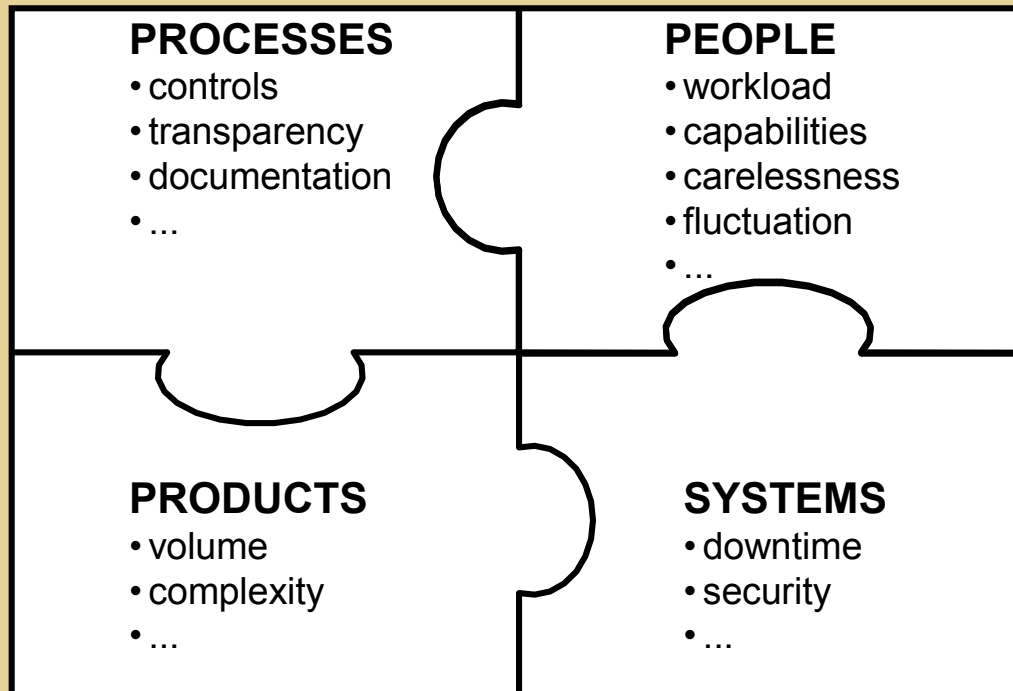
Internal Benefits	External Benefits	Commercial Benefits
<ul style="list-style-type: none"> • Culture <ul style="list-style-type: none"> • Better understanding of OR losses • Increased risk awareness • Management <ul style="list-style-type: none"> • Ability to manage OR losses within an expected range • Risk prioritization • Cost effectiveness of control • Continuous improvement vs. ad hoc / reactive improvement • Control <ul style="list-style-type: none"> • Transparency of controls • Framework for management process 	<ul style="list-style-type: none"> • Adherence to regulatory and legal requirements • Protection of Reputation • Positive influence on rating • Best practice implementation • Service Quality Improvement • Preservation of Capital 	

Classification of Methodical Sophistication for the Assessment of Operational Risk



Definition of Operational Risk

Operational risk can be found in all parts of the organization and is difficult to define ...



Categorization of Operational Risk

A thorough analysis of the underlying causes of operational risks is key to their differentiation and categorization. We categorise by underlying cause of loss for both technical and business reasons ...

Categories

Unauthorised activities:

Losses from unauthorised trading, overstepping authority or unauthorised approvals

Management process:

Losses due to failure in management processes (negligence or judgement errors specific to the management of operational risk)

Technology:

Losses due to failure or inadequacy of internal hardware / software

Criminal:

Losses from criminal / fraudulent activities (e.g. insider trading, theft)

Human resources:

Losses from poor judgement with respect to compensation & benefits, wrongful termination and discrimination

Disasters:

Losses due to natural catastrophes (e.g. floods, earthquakes) and accidental catastrophes (e.g. fires)

External environment:

Losses due to changes in political, legislative or regulatory factors

Transaction processing:

Losses from processing failure, poor documentation and erroneous data entry

Sales practices:

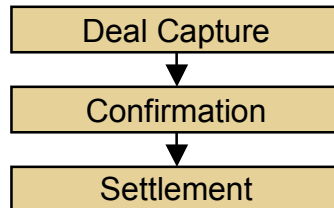
Losses due to inappropriate dealings with customers (e.g. deceptive sales practices, overcharging)

**There is currently
no generally accepted definition
of operational risk**

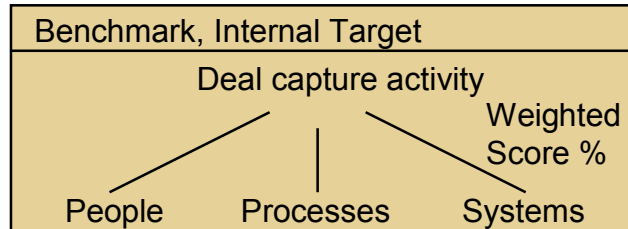
Tools Supporting Operational Risk Management (1/2)

Tools

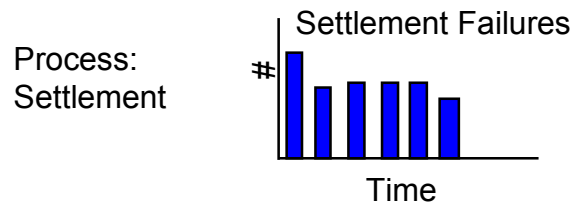
Risk Maps/ Process Flows



Qualitative Risk Assessment



Risk Indicators



Deliverables

- High level mapping of core internal processes
- Ratings of risks and controls
- Identification of hot spots and process bottlenecks
- ...

- Self-assessment score
- Management report summary
- Risk mitigation plan
- Work plan for corrective action
- Assignment of responsibilities
- ...



- Statistics drive the communication and management process
- Monthly report with key indicators and trends
- Daily indicators
- Various stand alone reports
- ...

Tools Supporting Operational Risk Management (2/2)

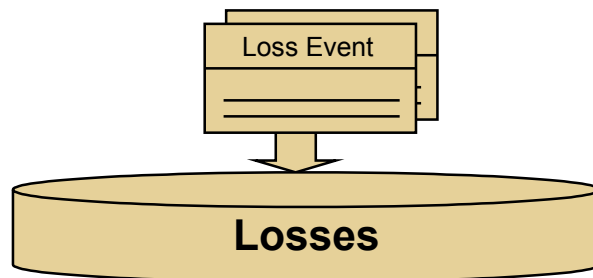
Tools

Escalation Triggers

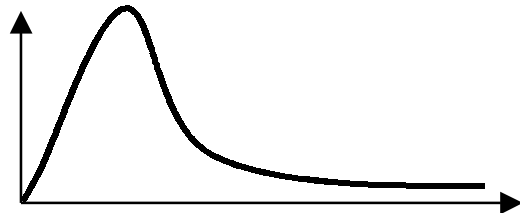
Quantitative or qualitative goals or limits for risk indicators that are used as a basis to communicate potential problems to a higher level management

Rating	Escalation Criteria
	_____
	_____

Loss Event Database



Quantitative Risk Assessment



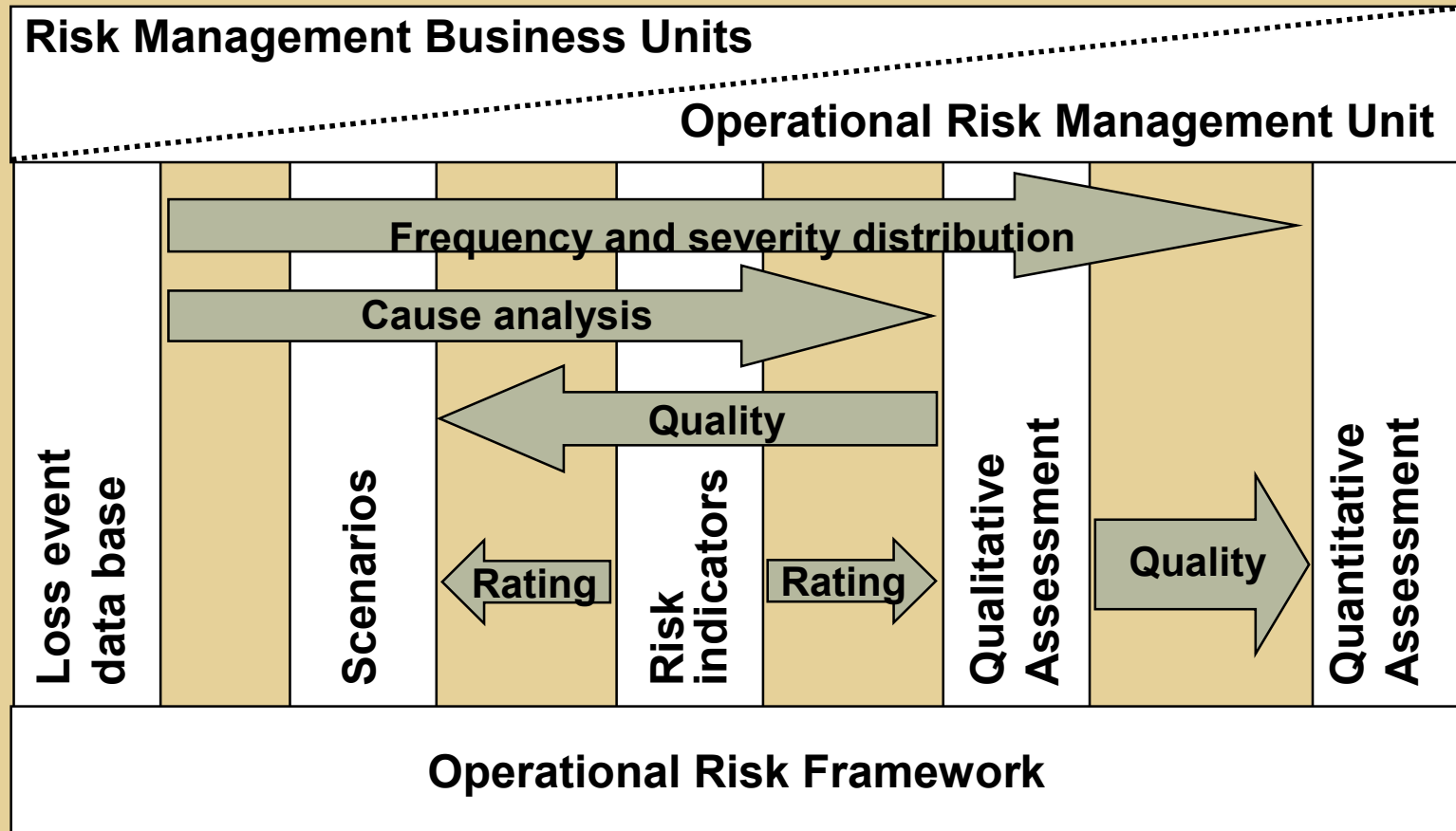
Deliverables

- Balanced scorecard for operational risk
- Enhancement of risk indicators
- Ticket/volume caps
- Error/exception rate caps
- Systems downtime caps
- ...

- Confidential database maintained by OR in conjunction with internal audit
- Historical loss profile (i.e. for quantification)
- External market data
- Loss cause analysis
- ...

- VaR for business lines and risk categories
- Capital/ cost allocation
- Cost/benefit analysis
- ...

Integrated Management of Operational Risks

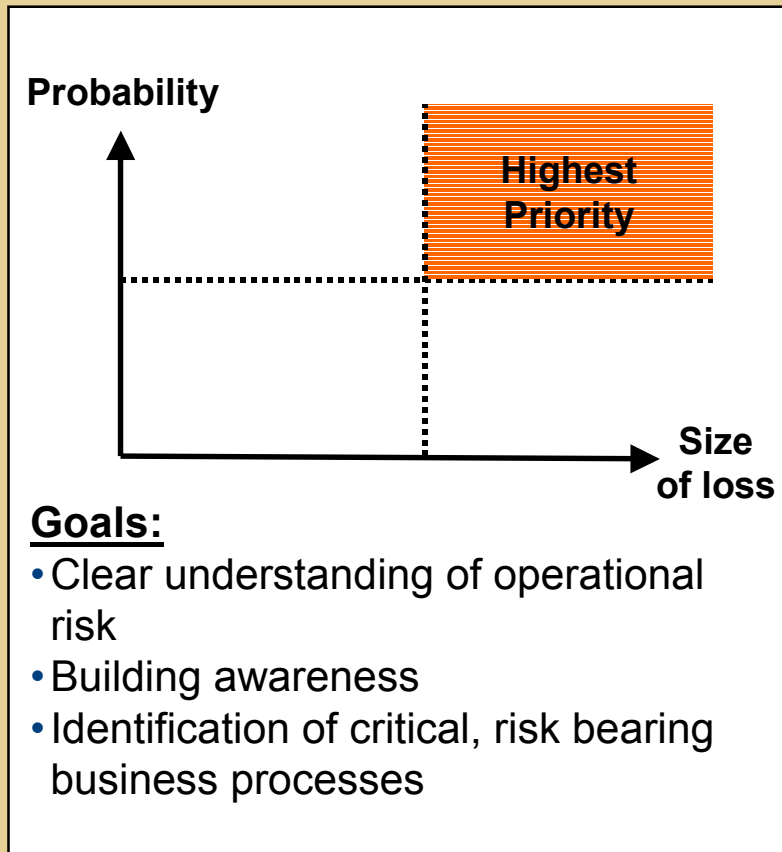


Quality

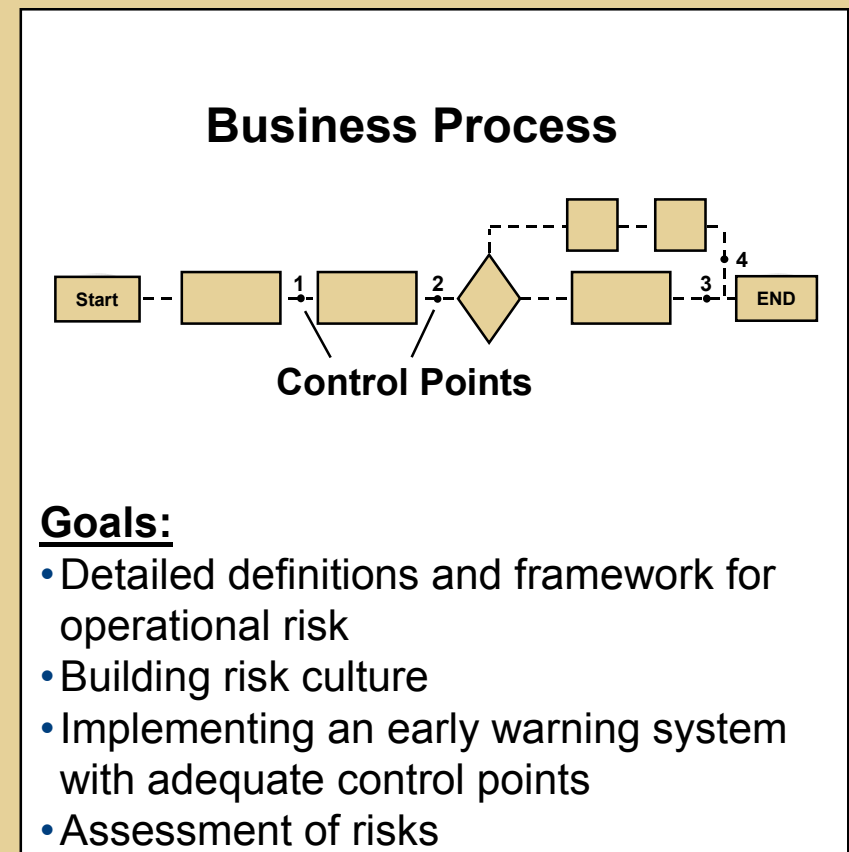
- Introduction
- **Qualitative Assessment**
- Quantitative Assessment
- Organizational Aspects of Operational Risk Management
- Lessons Learned

Qualitative Assessment: Process Oriented Approach to Operational Risk

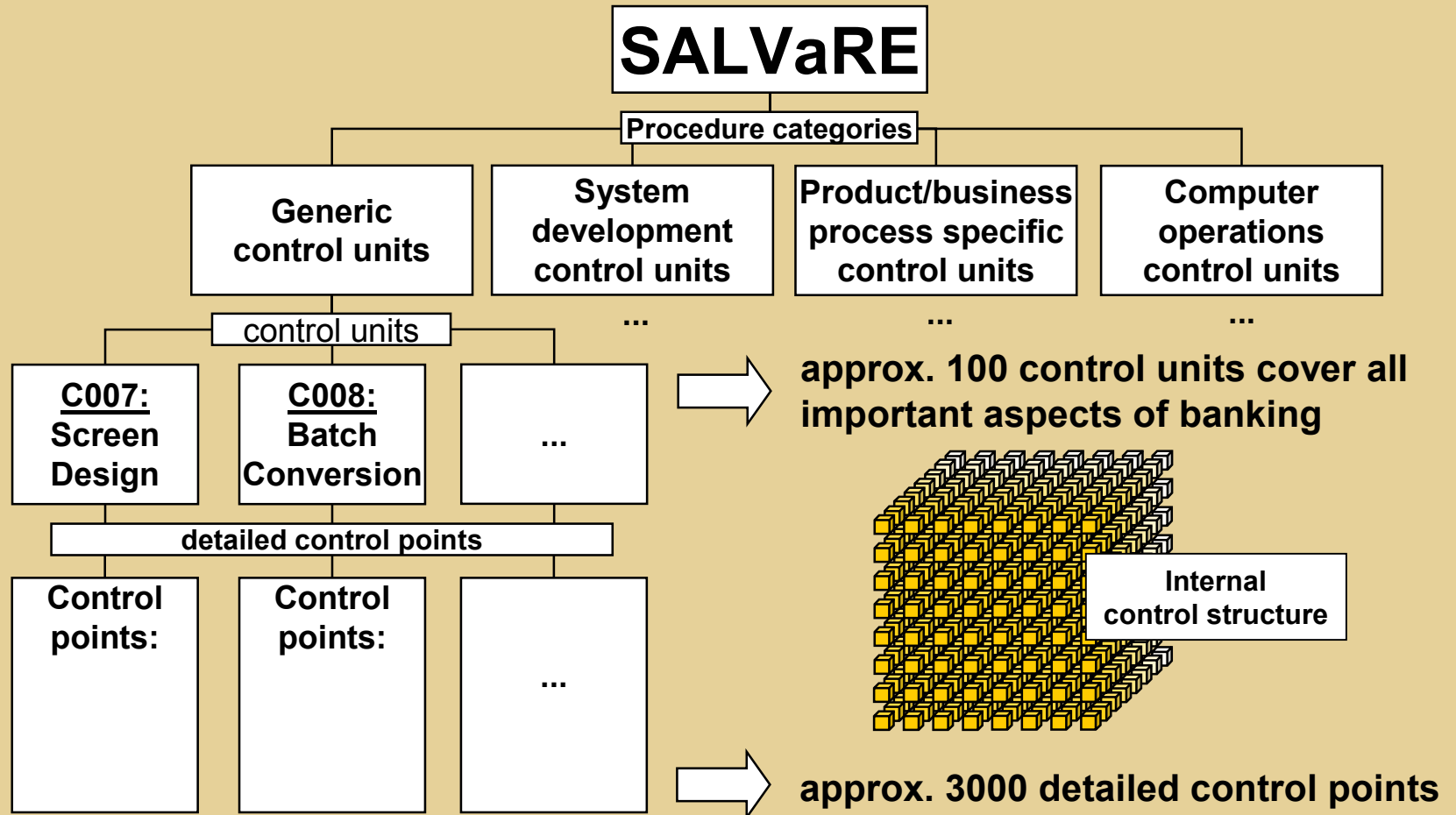
Step 1: Prioritization



Step 2: Detailed Qualitative Assessment

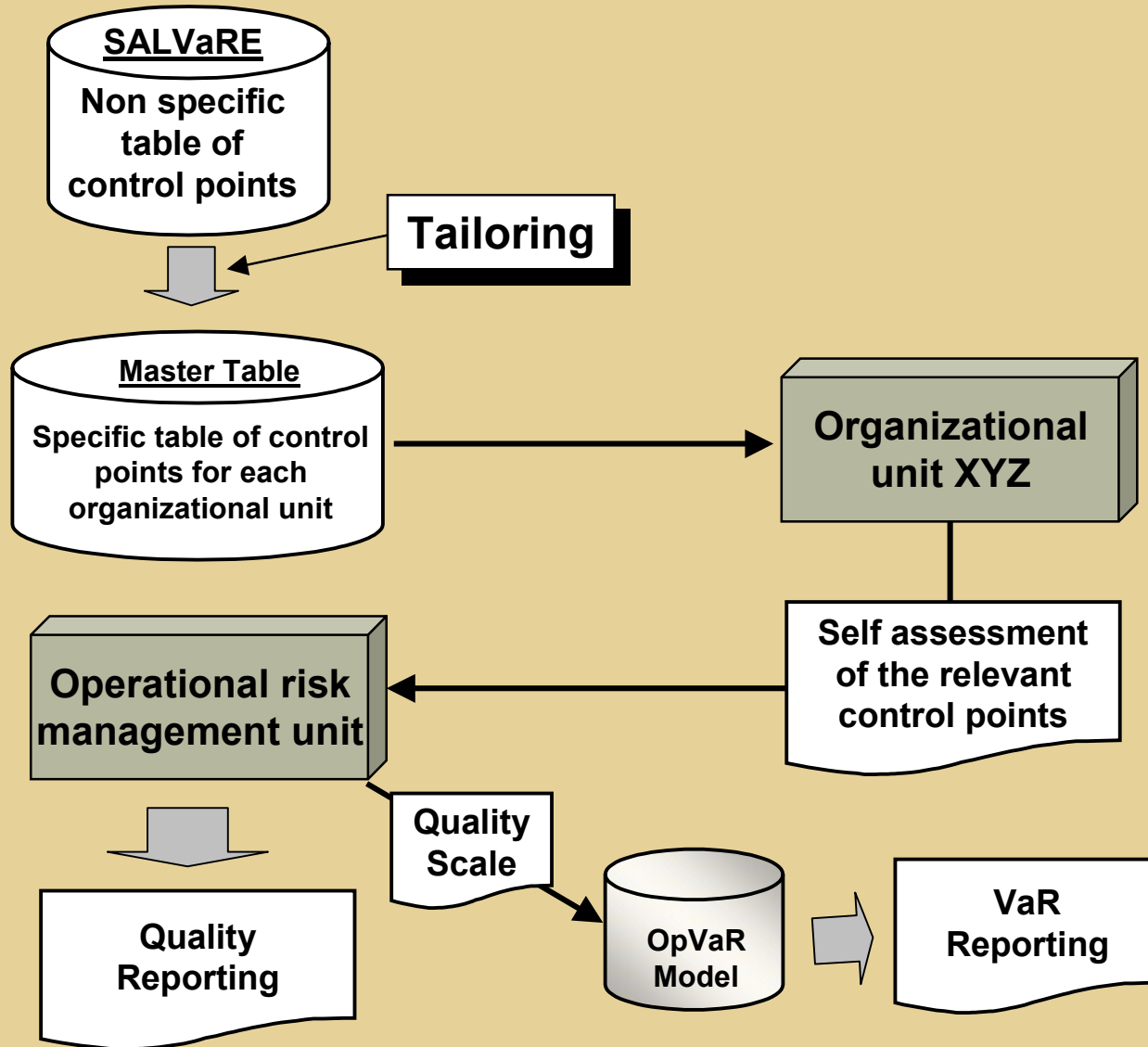


SALVaRE as a Methodology for the Qualitative Assessment of Operational Risk



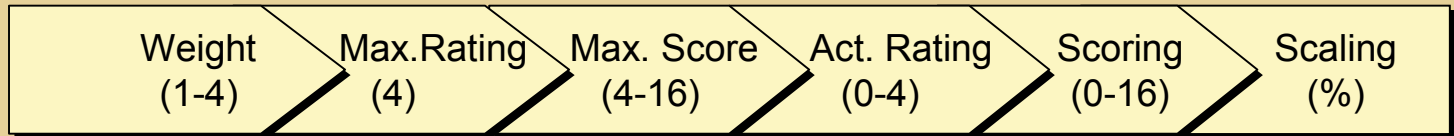
SALVaRE includes a large data base of best practice control points

SALVaRE: Basic Process of Qualitative Assessment



SALVaRE: Self Assessment at Control Points

ILLUSTRATIVE



$$4 \times 4 = 16 = 100\%$$

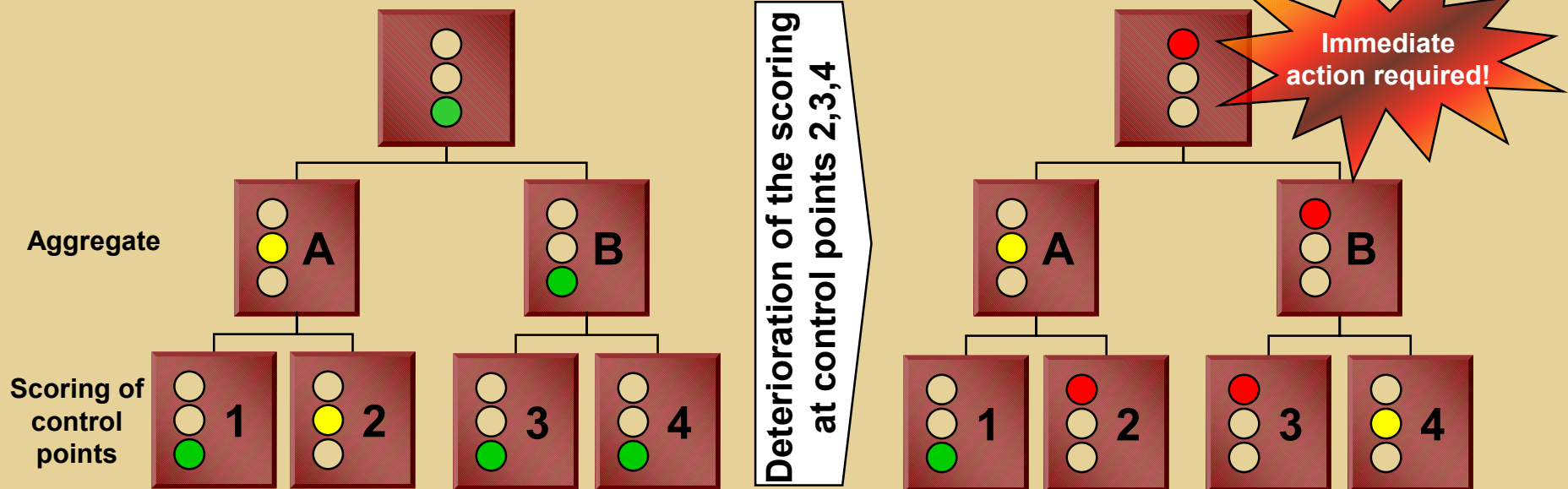
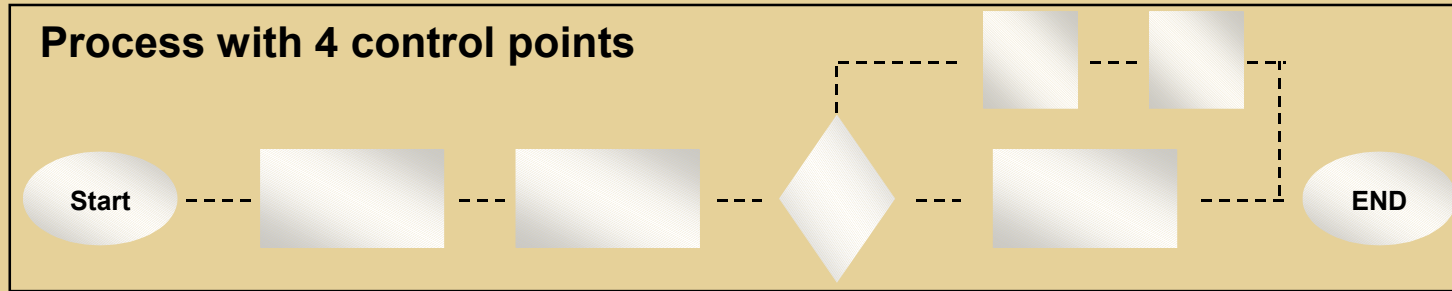
Control point 1: $4 \times 3 = 12 = 75\%$

Control point 2: $3 \times 2 = 6 = 50\%$

Control point 3: $4 \times 0 = 0 = 0\%$

Control Points	Weight	Max. Rating	Max. Score	Actual Rating	Actual Score	Scale	comments
1. Is this a new kind of project?	4	4	16	3	12	75%	
2. Are the project goals consistent and well documented?	3	4	12	2	6	50%	
3. Has the budget for the project been allocated?	4	4	16	0	0	0%	

Integration into the Business Environment



- **Introduction**
- **Qualitative Assessment**
- **Quantitative Assessment**
- **Organizational Aspects of Operational Risk Management**
- **Lessons Learned**

Creates Management Awareness:

- Necessitates development of a rigorous operational risk management framework
- Highlights cost of operational failure (expected losses)
- Identifies largest exposures (unexpected losses)
- Provides framework for cost-benefit analysis

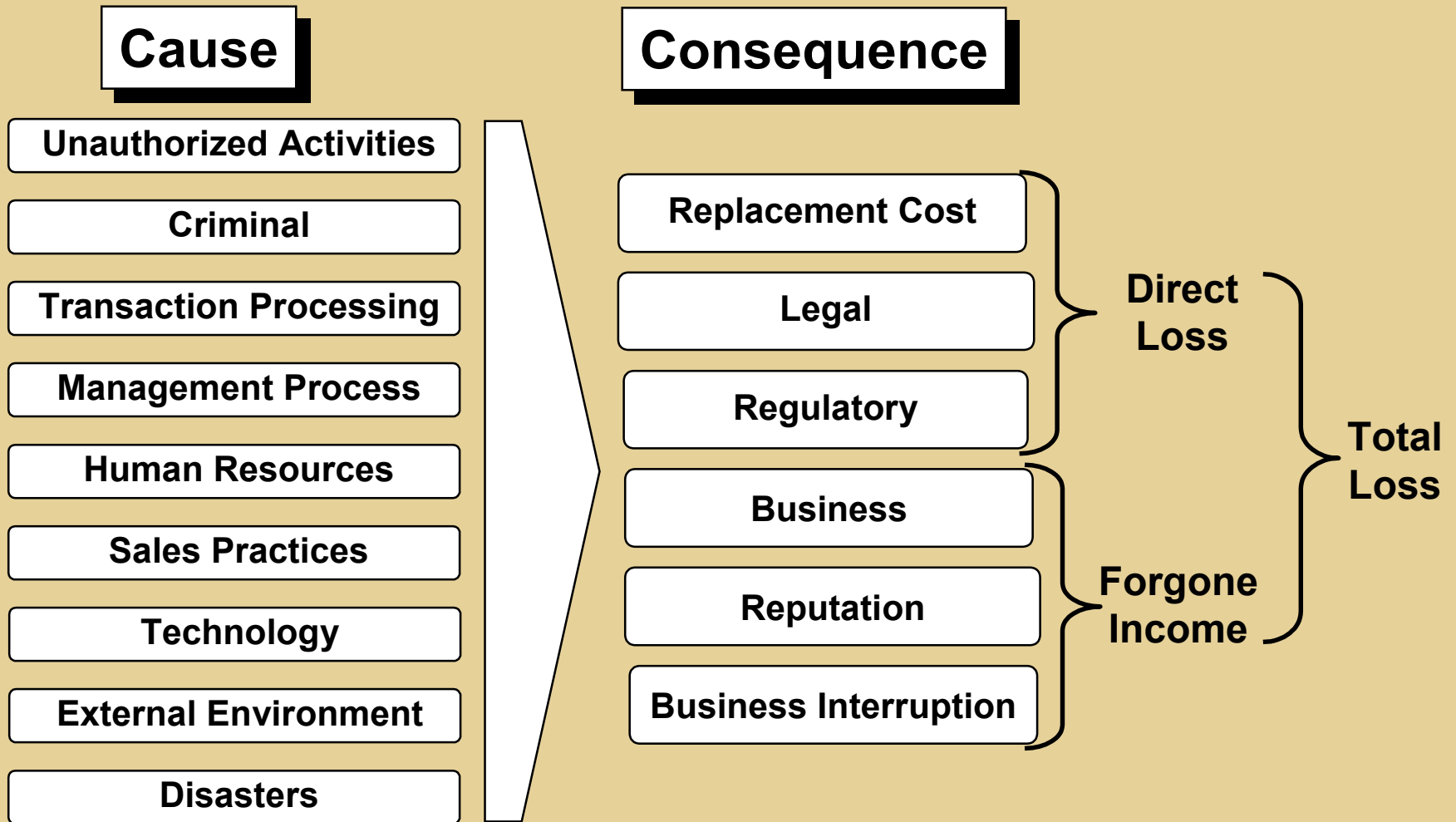
Links controls to performance measurement

- Quantifies operational risk capital
- Provides incentives for risk mitigation initiatives

Rationalizes Insurance Programs

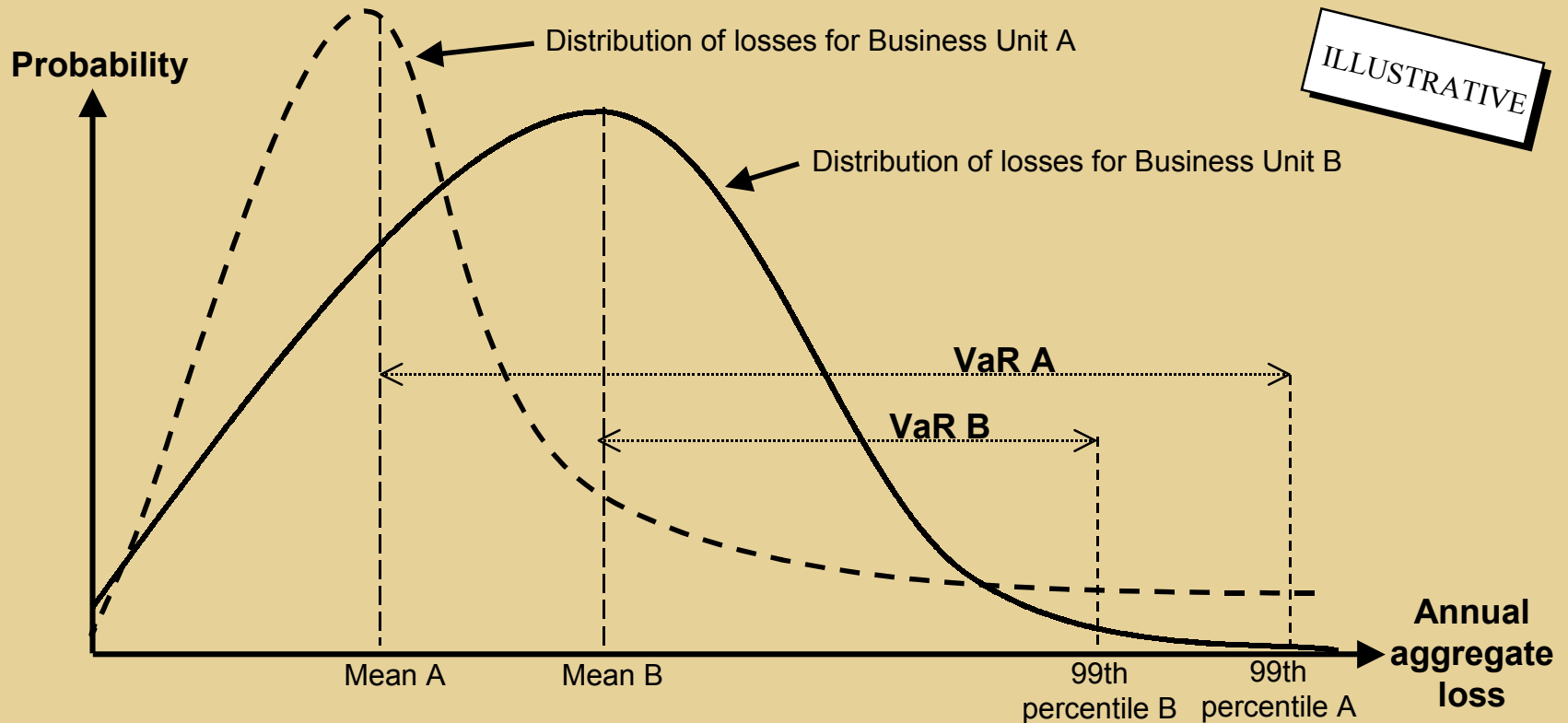
- Quantifies cost/benefit of alternate types of coverage

Categorisation by underlying cause



Operational Value at Risk

Operational Value at Risk (VaR) is the difference between the annual aggregate loss at a selected confidence level and the expected annual loss.

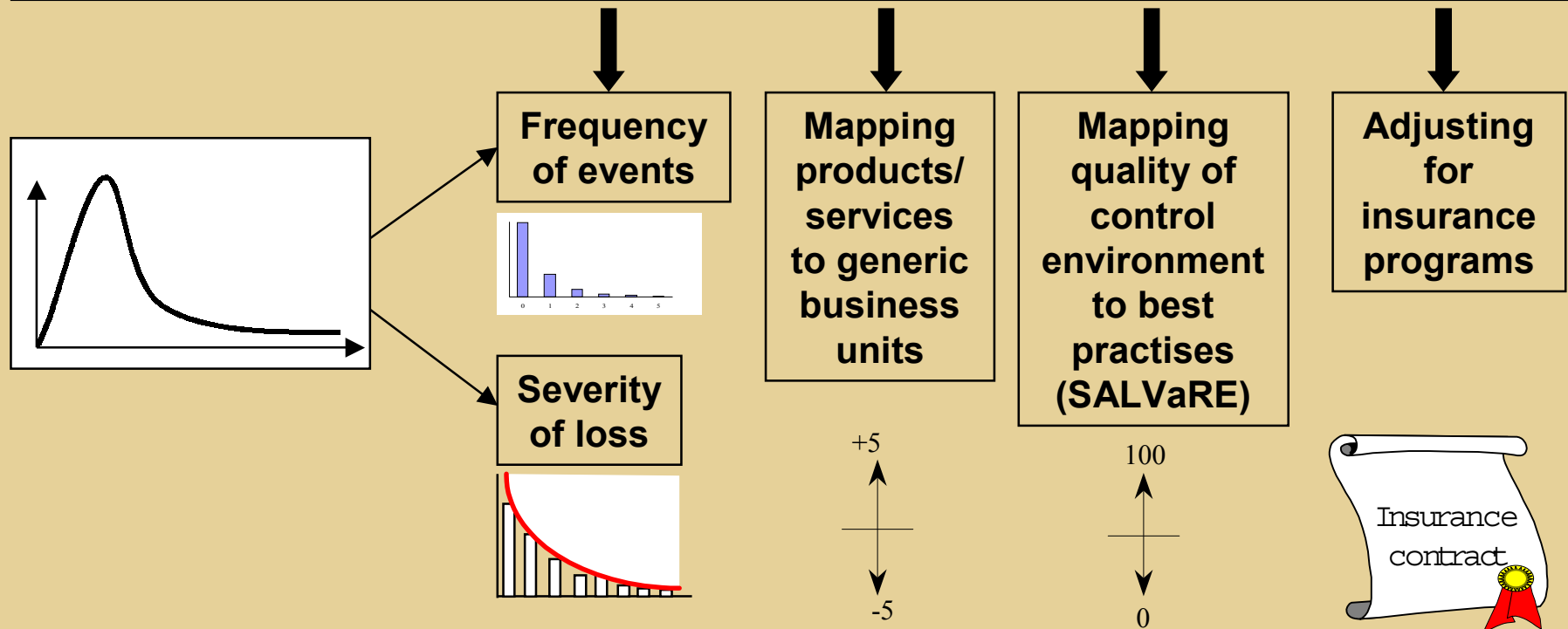


VaR is primarily driven by low frequency, high severity risks. Thus, some businesses which experience high annual losses may have a relatively low VaR.

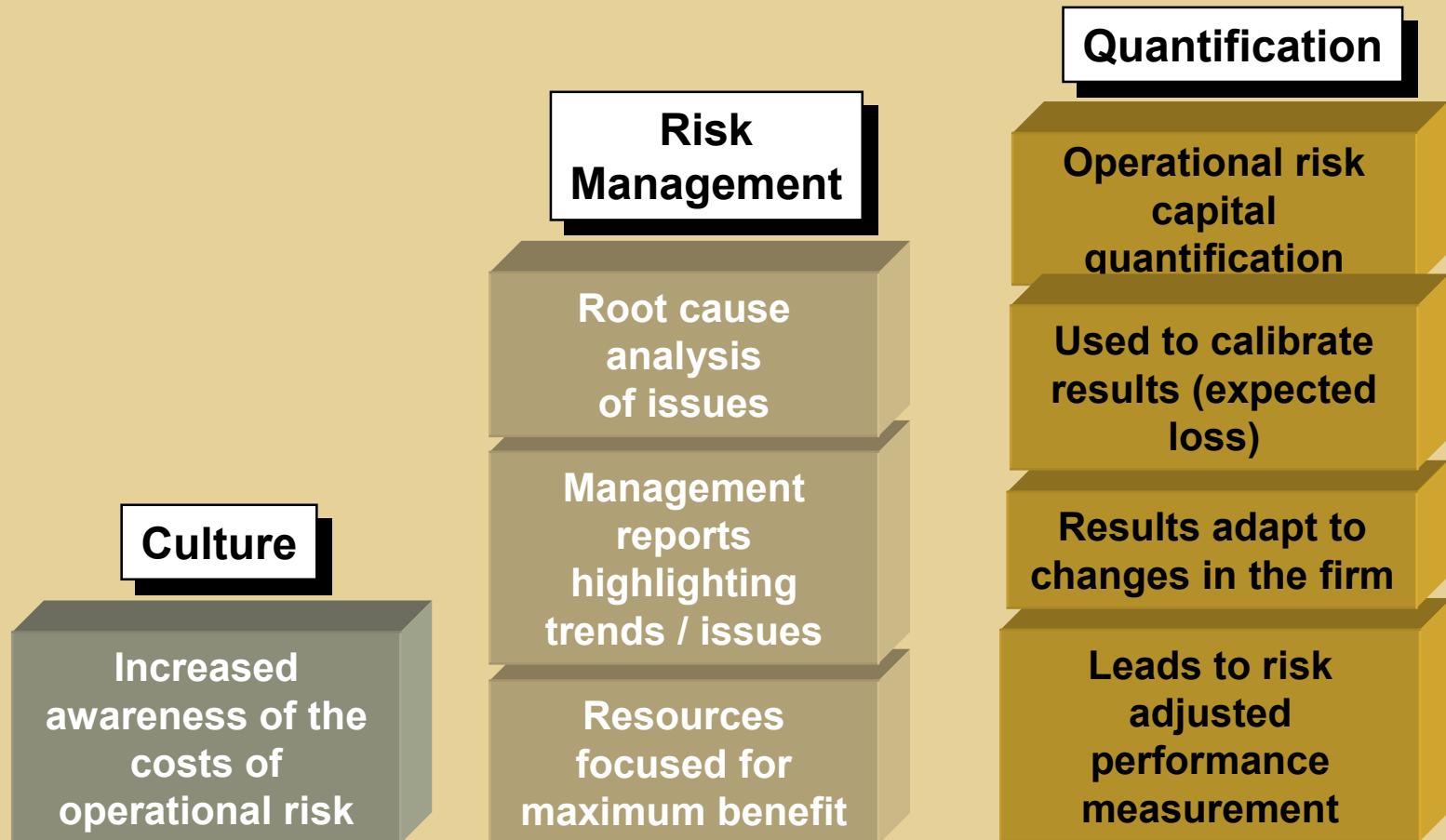
Overview of the OpVaR Approach

OpVaR is a statistical/actuarial approach which is based on the theory that historical data can be used to measure the full range of potential exposures each business faces.

OpVaR = $f(\text{Exposure, Relevance, Quality, Transfers})$



Collection of loss data will provide significant commercial benefits, since it leads directly to the quantification of operational risk and the development of management processes.

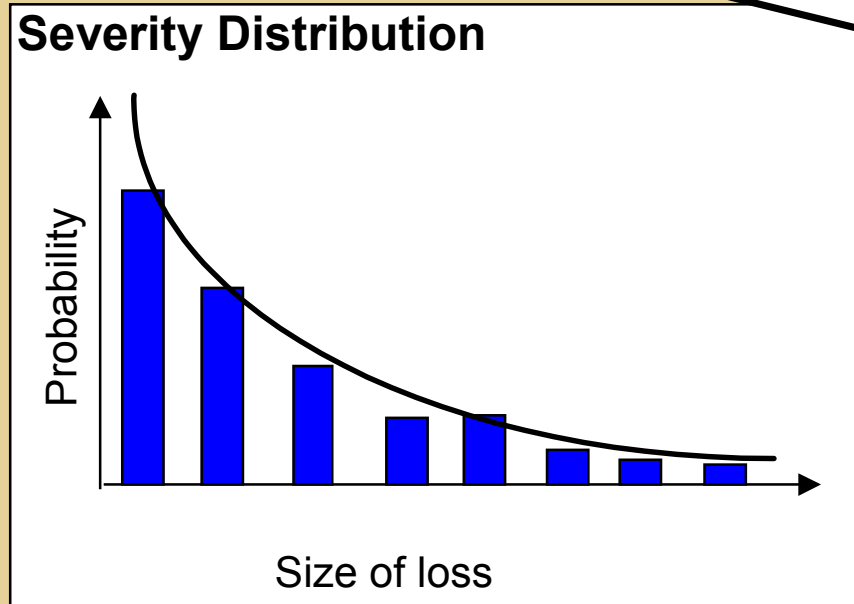
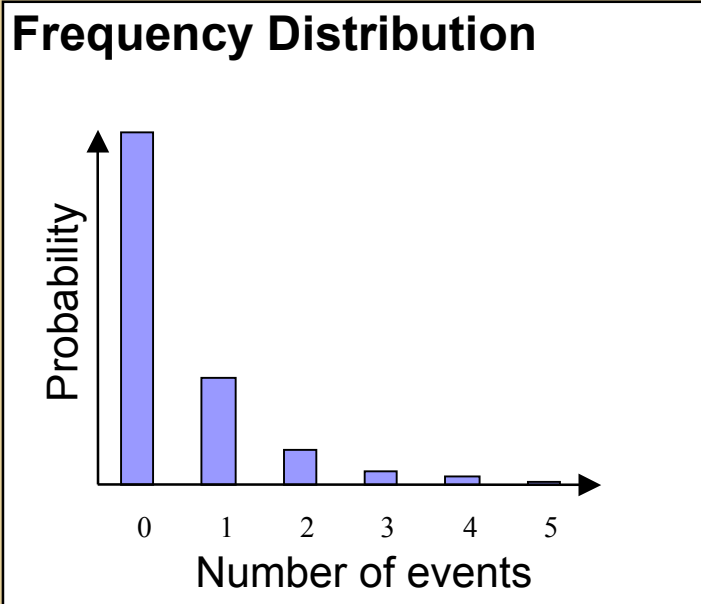


Customized Distributions

Loss data is used to calculate the risk profile of each business, i.e., the inherent exposure of each business to each risk category. The end result is a customization set of frequency and severity distributions for each business unit, for each risk category.

Business unit: Retail Banking
Risk Category: Criminal

ILLUSTRATIVE



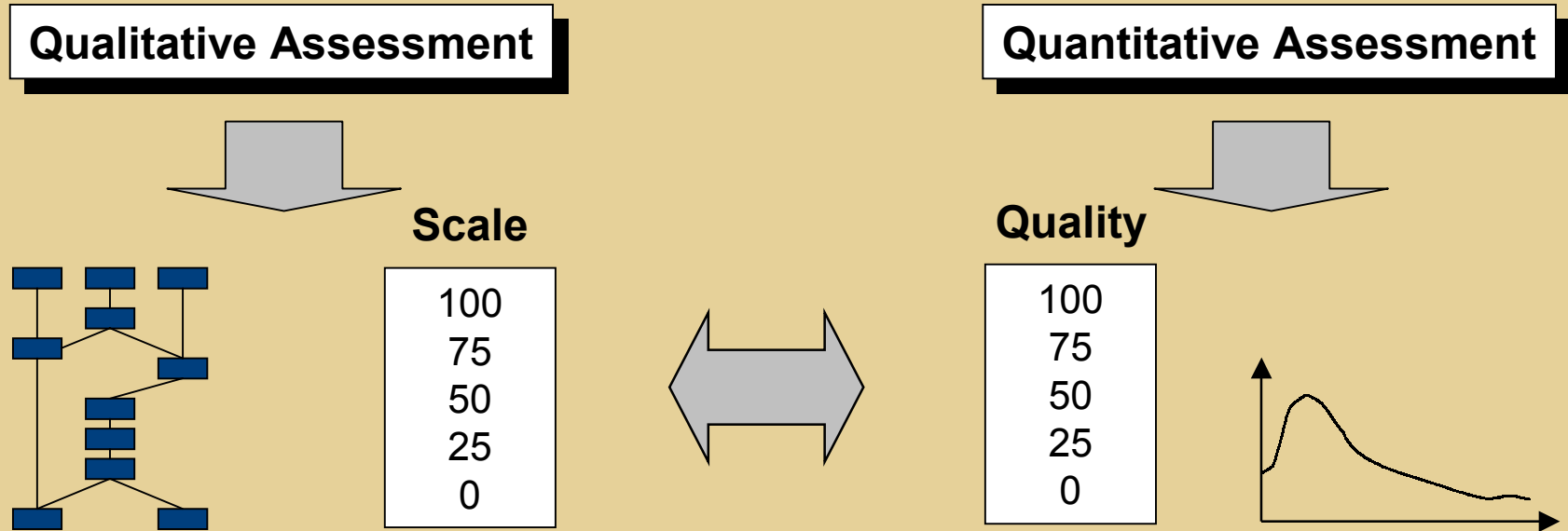
Aggregation of OpVaR

OpVaR's bottom-up approach results in a VaR figure for each business line and risk category on a diversified and undiversified basis.

	Unauthorized Activities	Sales Practices	Criminal	Total
Retail Banking	56	73	40	246
Commercial Banking	74	87	65	345
Trading	468	123	11	543
Asset Management	235	89	5	388
⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮
Sum	944	224	145	1,825
Total	567	156	89	1,256

ILLUSTRATIVE

Integration of the Qualitative and the Quantitative Assessment of Operational Risk

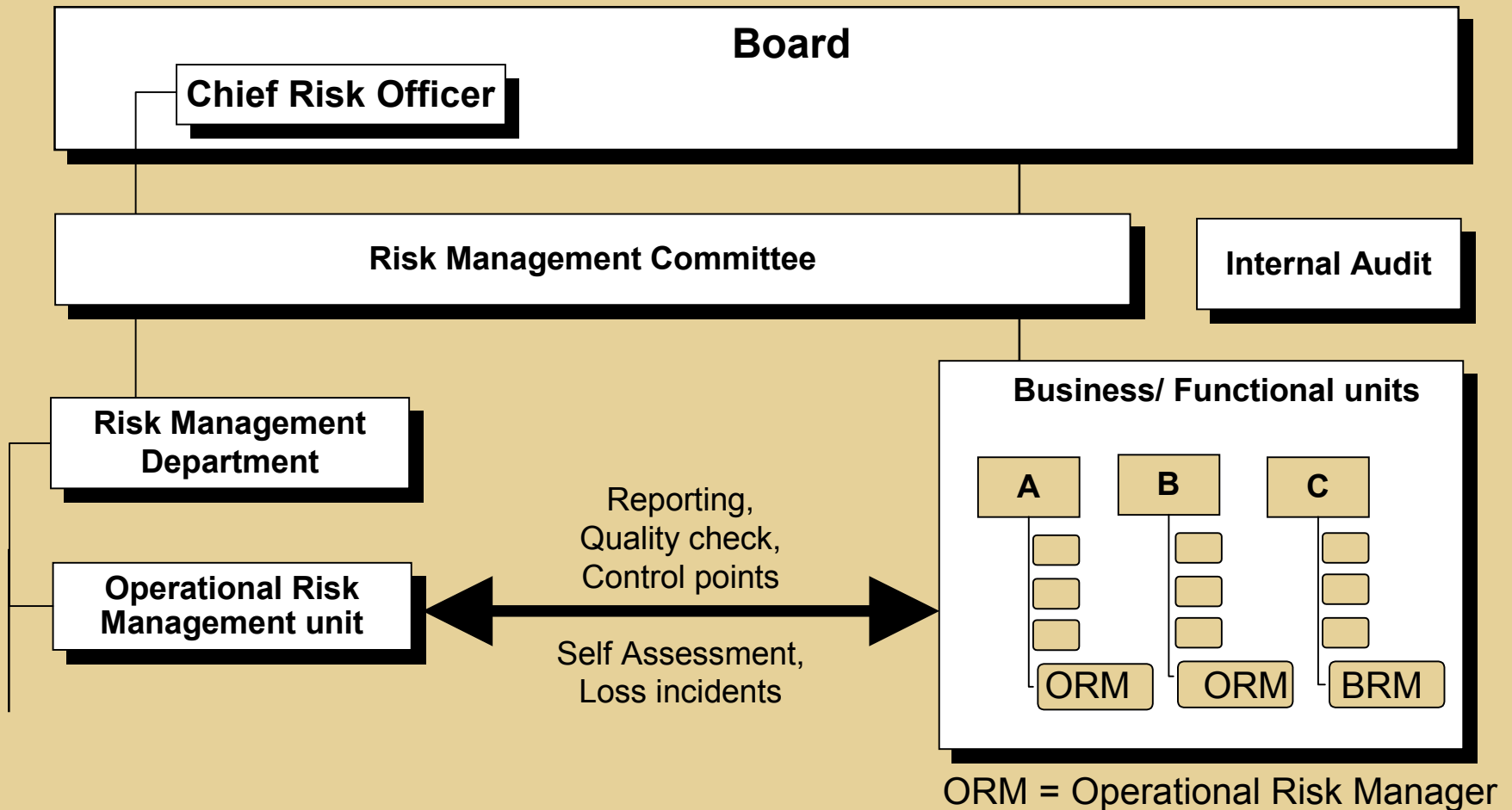


The scale value from a qualitative assessment directly drives the quality parameter of the OpVaR model and hereby links historical data with future scenarios.

Table of Contents

- **Introduction**
- **Qualitative Assessment**
- **Quantitative Assessment**
- **Organizational Aspects of Operational Risk Management**
- **Lessons Learned**

Centrally Driven Operational Risk Management Structure



ORMs are appointed by the business/ functional unit leader and work closely with the operational risk management unit.

Operational Risk Reporting

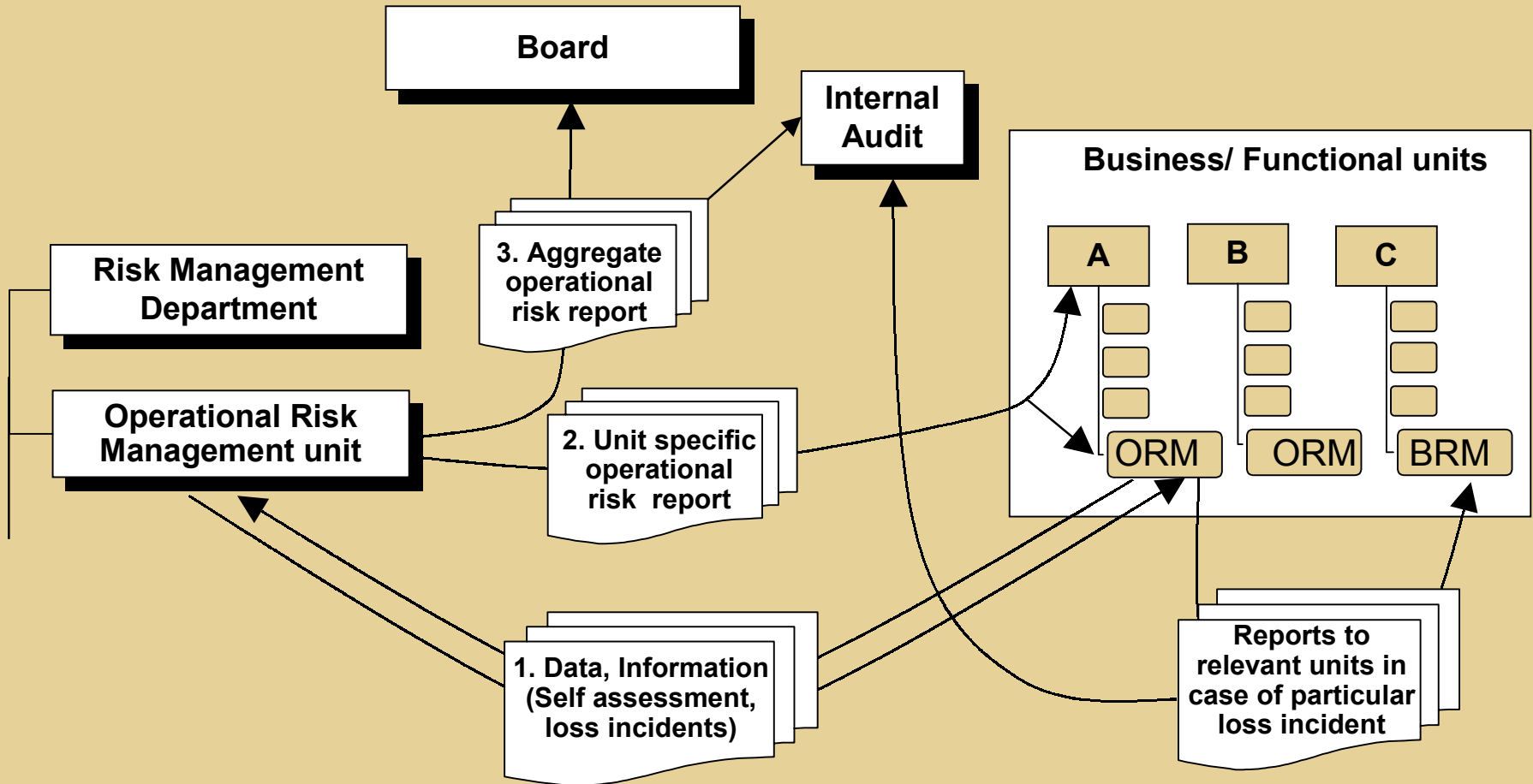


Table of Contents

- **Introduction**
- **Qualitative Assessment**
- **Quantitative Assessment**
- **Organizational Aspects of Operational Risk Management**
- **Lessons Learned**

Approach to Operational Risk Management (I)

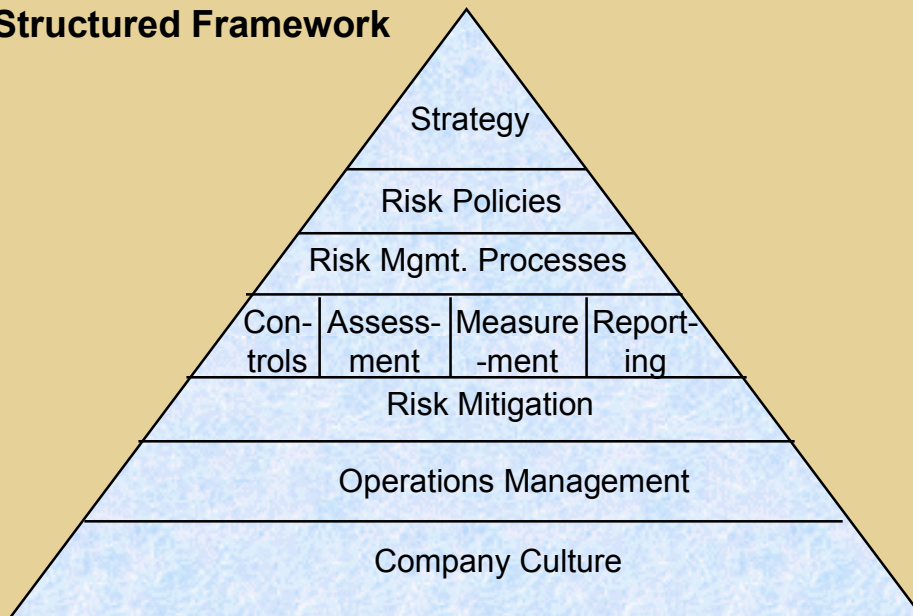
Value Added

- Quality Management
- Improved system performance & contingency, organizational structure and processes
- Improved ratios (risk/return, cost/return)

Group Wide

- All legal entities - subsidiaries and branches / business divisions and support functions

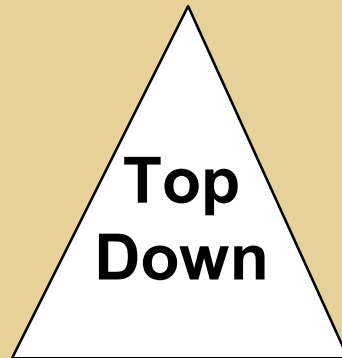
Structured Framework



Centrally coordinated

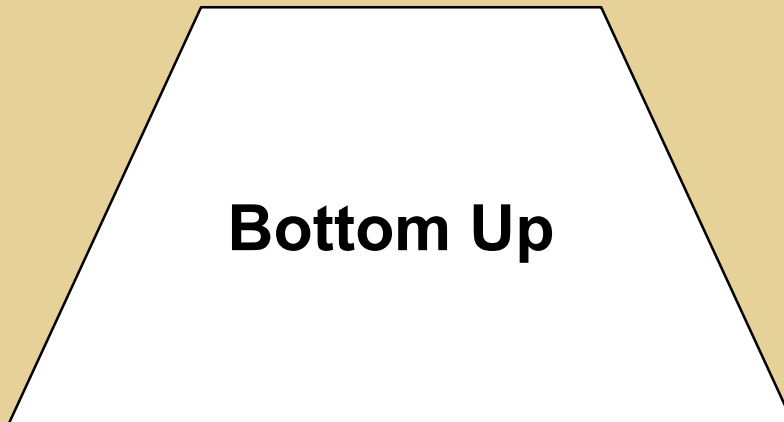
- Central program management
- Top management commitment
- Clear project structure
- Leveraging of know how

Operational Risk Management should incorporate top down and bottom up approaches



Top Down:

- Group operational risk committee (and sub-committees)
- Provision of Central Framework
- Specialized Operational Risk Unit
- Coordination of activities, procedures and methodologies
- Risk Profiling & Capital Allocation
- Benchmarking



Bottom Up:

- Identify and collect relevant data
- Local operational risk committees
- Generate and share best practice
- Business specific policies
- Process methods
- Self assessments

- Show a value proposition to the business/ functional units
- Buy in the management of the business/ functional units
- Take your time to build awareness for operational risk
- Don't overwhelm business with cumbersome and rigid control systems
- Start collecting loss data early on