2025 KOnnect

Integrated Scenario Analysis and Common Impact Drivers

SPEAKER

Dr. Ariane Chapelle

Partner, BDO Belgium

CONNECTING RISKS THAT MATTER

Outline

1. Scenarios: a Must-Have?
2. Simpler than you think: Identifying Common Impact Drivers
3. Standardizing Scenario Assessment: Example of a Uniform Template

My Short Bio (regarding scenario analysis)

2000

Active in Risk Management since 2000

2007

Studying large events & scenario analysis since 2007

2013 - 2023

UCL Honorary Reader in Operational Risk Measurement (2013 – 2023)

What is the status of Scenario Analyses and Assessments in your organization:

We don't use scenario analysis	0%
We identify plausible extreme events, but we don't quantify them	0%
We perform a full scenario analysis, but we would like to improve quantification	0%
We perform mature scenario analysis and quantification	0%

0 total participants | 0 votes

Scenario Analysis: the reasons to postpone

- *It's a nice-to-have*
- *We'll get to it later; there are more urgent priorities*
- *These are very unlikely events, anyway*
- *It's only for regulatory capital purposes*
- *It's impossible to quantify*
- *We have a BCP / an ICT plan, we're fine*
- *It's depressing to think about catastrophic events*

Does any of these reflections sound familiar?

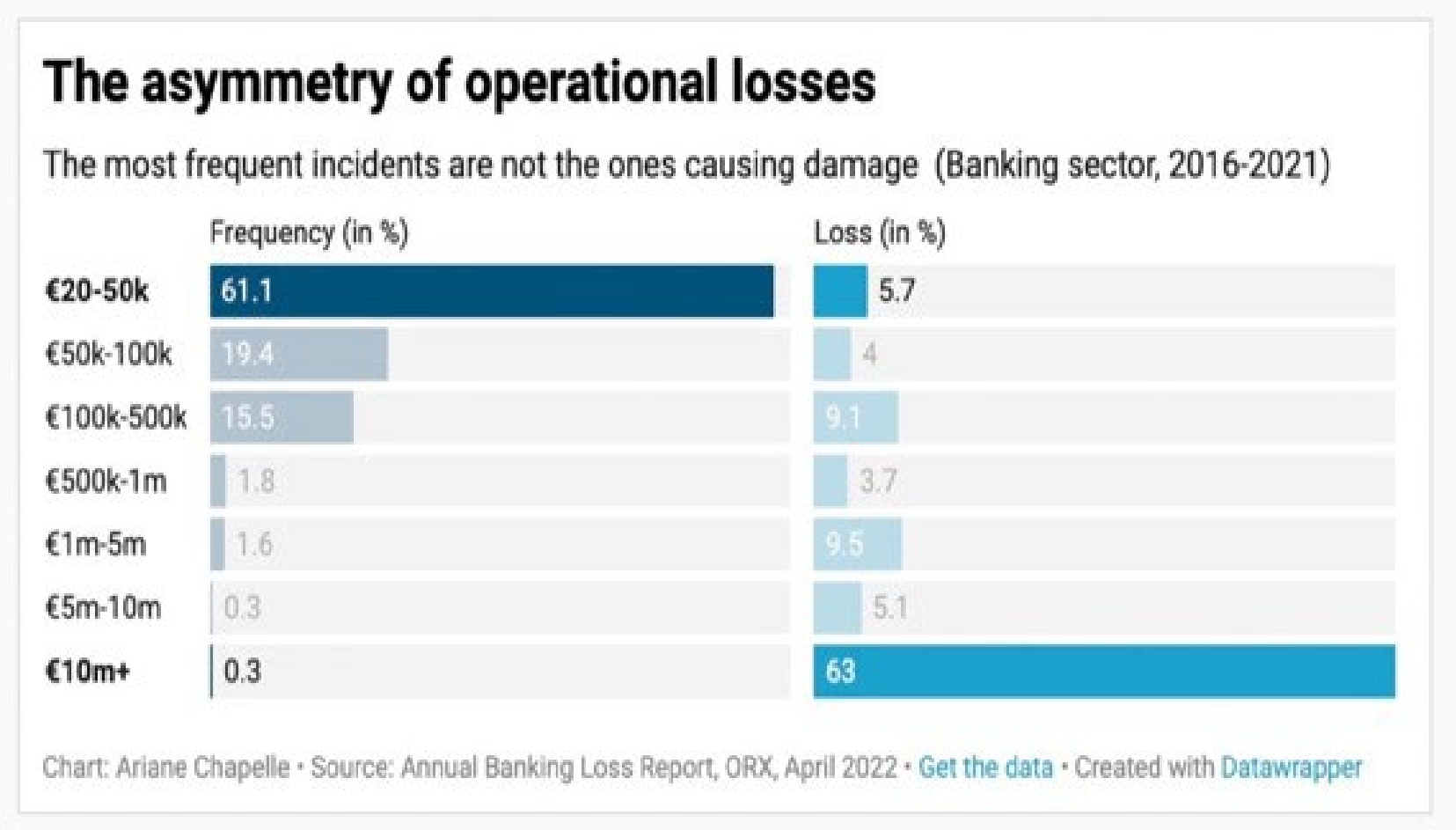
2025 KOnnect

Scenarios: a Must-Have?

The Benefits of Scenario Analysis

CONNECTING RISKS THAT MATTER

Are “Rare Events” so Rare?



- Disruptions
- Data breaches
- Ransomware
- Fires
- Frauds
- Fines
- Accidents
- ...

0.3% of 65,000 incidents collected per year = about 200 incidents of €10m+ per year, for 100 members = 2 scenario events per organisation and per year, on average.

Rarity of incidents depends on control effectiveness

Scenario Analysis: a Must-Have!

- Benefits
  - Awareness
  - Control assessment and testing
  - Preparedness
  - Operational Resilience (with proper plans)
  - Financial Resilience (with proper capital levels)
  - Compliance

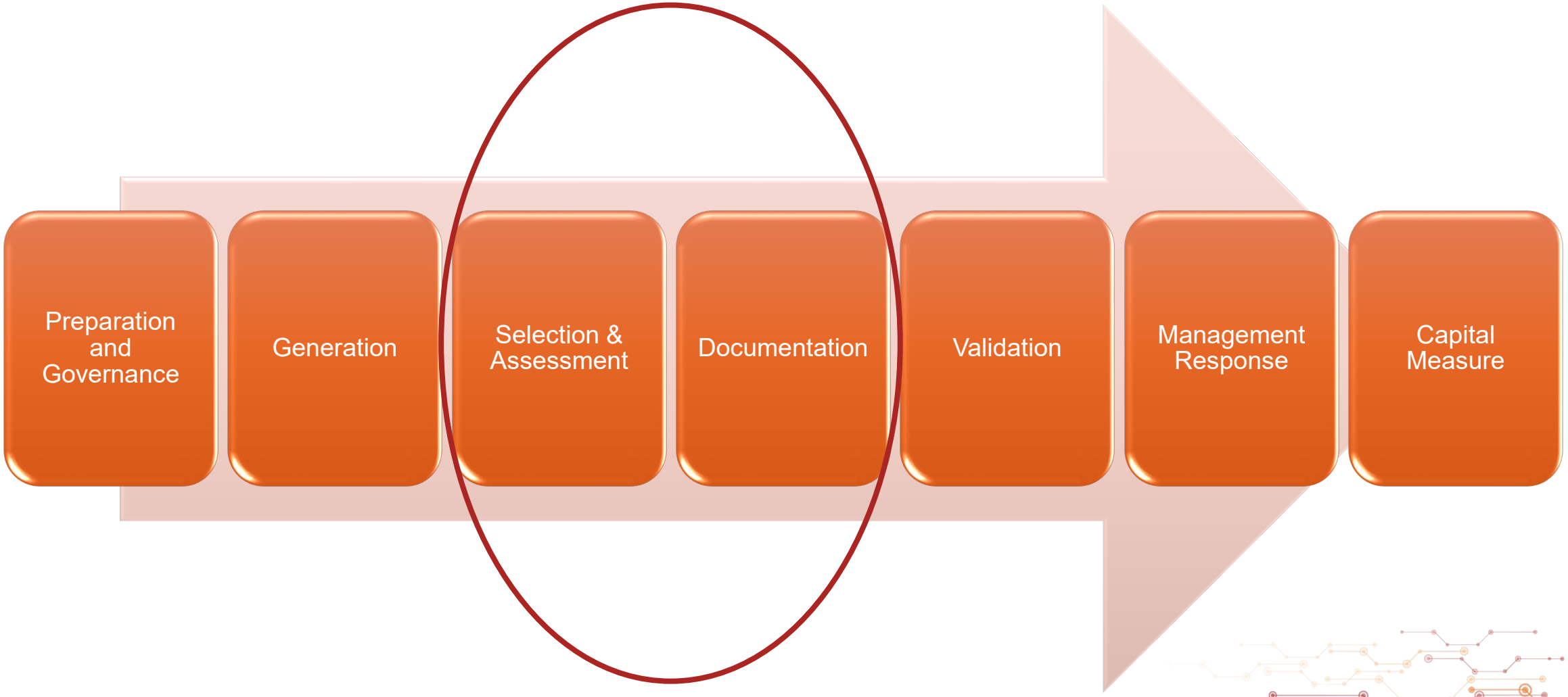
2025 KOnnect

Simpler than you think

Identifying Common Impact Drivers

CONNECTING RISKS THAT MATTER

Seven Steps of Scenario Analysis



Structured Scenario Analysis

- Most scenarios can be decomposed into the same impact types
- Similar assessment structures allow for
  - Comparison, for prioritisation
  - Explanability of results, for action plans if needed
  - Assessment of losses at higher probabilities :50%, 20%, 10% for instance

Impact types for most scenarios

1. **Damage to material or immaterial assets** (data centre, building, IP...)
   - % destruction * replacement value
2. **Loss of business due to disruption**
   - Revenue per unit of time * duration of the event (detection + duration)
3. **Remediation costs** (crisis management, investigation & repair, monitoring & reporting),
   - Internal man-days ($1k/day) + external services + further remediation programs
4. **Stakeholder impacts**
   - Customers & staff attrition, regulatory sanctions, suppliers' changes in prices and services, reputation damage, legal costs

2025 KOnnect

Standardizing Scenario Assessment

Example of a Uniform Template

CONNECTING RISKS THAT MATTER

Simple and Structured Scenario Assessment

= Decomposing a scenario (Example: Data Breach)

1. **Into impact factors or drivers, such as:**
   - Time to detection * volume of data leaked / time * value per data / vol.
   - + remediation cost (repairs, consultants, management time)
   - + communication and stakeholders' impacts (customers, regulators,...)
2. **At a range of values (Low – Medium – High – Extreme)**
3. **For different likelihood levels (60% - 30% - 8% - 2%), with values dependent on the controls in place and their effectiveness**

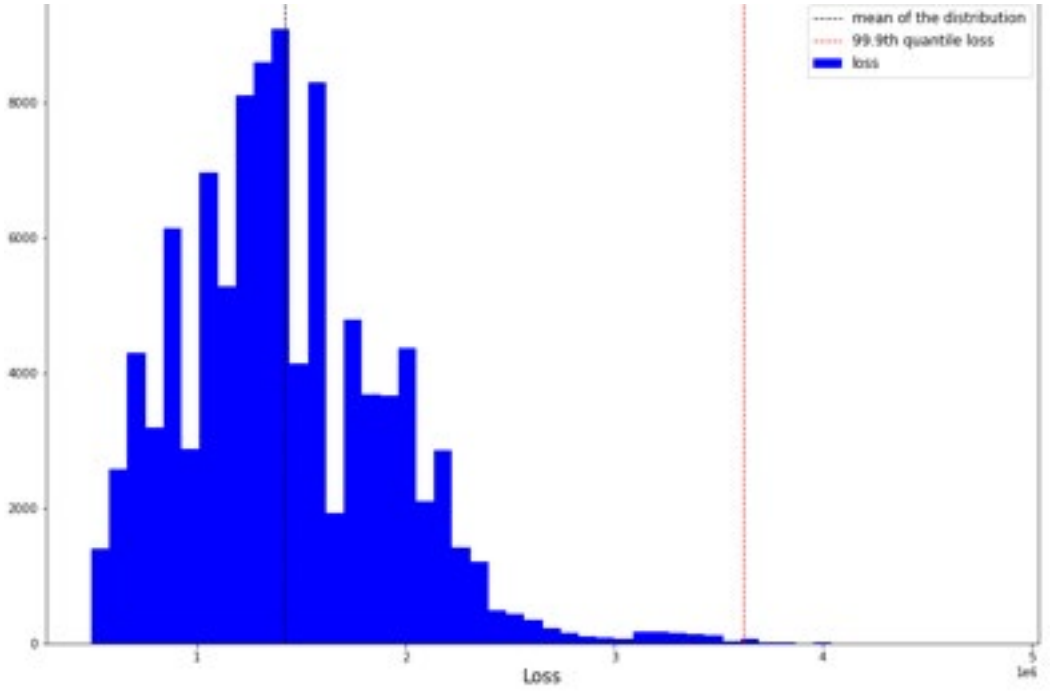
Standardized Template

Text Presentation
Scenario Title Ex: Data breach
Rationale Why selected
Scenario Exposure Data type held & value
Control Environment Key controls and responses

Quantification	L	M	H	E
Direct value loss	$	$	$	$
Time (detection + disruption)				
Volume per time				
Value per volume (physical / digital assets)				
Remediation cost	$	$	$	$
Investigation time				
Communication time				
Man-day value				
External services				
Stakeholders impact	$	$	$	$
Customers attrition				
Customer value				
Regulatory sanctions				

Assessment and Quantification – Example

Quantification	L	M	H	E
Direct value loss (k$)	**40**	**600**	**14,400**	**80,000**
Time (detection + disruption) (in hours)	2	8	72	400
Volume per time (Gb / m3)	20	50	100	100
Value per volume (physical / digital assets)	1,000	1,500	2,000	2,000
Repair cost (k$)	**-**	**210**	**1,000**	**2,750**
Investigation time (in days)	0	100	400	600
Communication time	0	10	100	150
Man-day value ($)	1,000	1,000	1,000	1,000
External services (k$)	0	100	500	2,000
Stakeholder impact	**-**	**350**	**7,000**	**25,000**
Customer attrition	0	100	2,000	5,000
Customer value	3000	3000	3000	3000
Regulatory sanction (k$)	0	50	1,000	10,000
Total	**40**	**1,160**	**22,400**	**107,750**



What good looks like

- Quarterly TDRA: *Top-Down-Risk-Analysis* at Executive level
- Active business implications in the assessment process
- Reporting at all levels of likelihood (not only 99.9)
- Linked to strategic decisions (key projects, expansions, etc.) and budgeting (mitigation costs, expected losses and capital needs)

Conclusion and Summary

- Scenario identification and assessment are essential components of a risk management framework.
- “Rare” events are more common than many believe, and they are brewing certainties in weak control environments.
- Structured scenario assessments are effective methods to identify common impact drivers and heightened risk exposures.

After this talk, are you more likely to revisit your scenario analysis practice?

Yes, definitely.	0%
Maybe, I will consider it.	0%
No, I don't think so.	0%
We already use a similar approach.	0%

0 total participants | 0 votes

2025 KOnnect

Questions?

CONNECTING RISKS THAT MATTER

Connect with me.

Ariane Chapelle

e: ariane.chapelle@gmail.com

t: +447833453854

w: https://arianechapelle.com/

in/ariane-chapelle-985b19/

2025 KOnnect