Banking

Ana Lacerda

Fall Semester 2024

Course: Banking [2206]

Operational risk

Disclaimer: The views expressed are my own and do not necessarily represent the views of Banco de Portugal.

To be covered today

- Operational Risk

Operational Risk

Operational Risk started to be addressed at the technology level:

- banks are large investors in IT systems;
- an error might have incredible costs (what about a miscalculated price in a large trade?);
- M&A in banking forced a lot of system integration, leaving systems more fragile;
- banks are suitable targets for hackers, as there is electronic money, and most clients will not notice an undue transaction in time.

Operational Risk

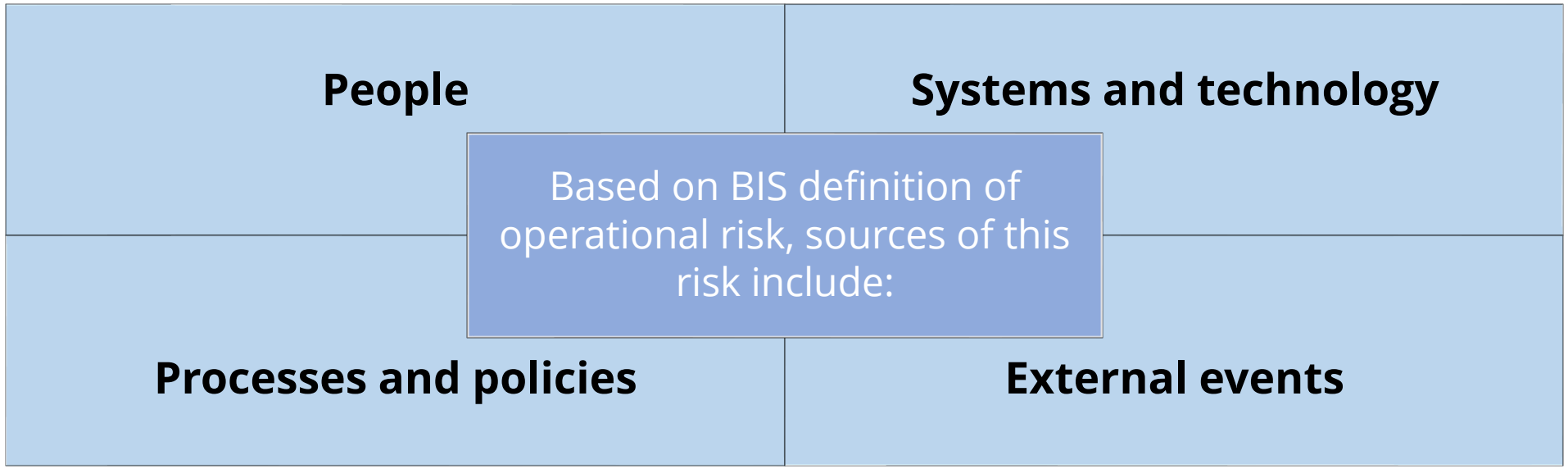
- Even with all the concerns of financial institutions, operational risk measurement only started to be addressed with Basel II.

- According to the Bank of International Settlements (BIS):

Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk,- but excludes strategic and reputational risk.

- It is embedded in all banking products and activities.

Operational Risk



These categories are related to one another and may be partially overlapping

Press Corner

Operational risk muscles into focus

© AFP

Brooke Masters NOVEMBER 25 2012

Of all the perils that banks face, operational risk is the most amorphous and the hardest to protect against.

Big capital reserves – any bank's main line of defence against risk – are helpful for absorbing losses from bad loans, but there is very little that a chunk of equity can do when a hurricane swamps the trading floor, a top trading partner goes bust or the ATM network goes down.

Protecting against operational risk "is about a lot more than capital. If you can't open your doors, all the capital in the world isn't going to help," said Julie Dickson, Canada's top banking regulator.

She is spearheading global efforts by the Financial Stability Board to improve supervision of the world's biggest banks, and last summer, operational risk muscled its way on to her committee's agenda.

Every time they met, a new kind of operational risk was leading the news. JPMorgan's massive trading loss and three weeks of computer woes at Royal Bank of Scotland were closely followed by the Libor rate-setting scandal and the UK banks' £10bn tab for mis-selling payment protection insurance.

Press Corner

Opinion **Risk Management**

How risk managers can survive a 'perfect storm'

It is vital to strengthen operational resilience and crisis management frameworks

EVGUENI IVANTSOV + Add to myFT

© Angelos Tzortzinis; Anthony Kwan; Anatolii Stepanov/Getty

Evgueni Ivantsov MAY 11 2022 6

As Winston Churchill once said: "If you are going through hell, keep going."

This is an extraordinary time for risk management professionals. In 2008, when the global financial crisis unfolded, risk managers found themselves trying to counter the biggest financial shock since the Great Depression of the 1930s. Today, the world is facing a greater challenge — three global crises at the same time: the public health crisis, the geopolitical crisis, and the climate change crisis.

Addressing risk amplification

These three crises show a high level of interplay which amplifies the severity of each — for example, the disruption of global supply chains due to Covid and war in Ukraine. This creates the conditions for a tail-risk event that could explode when several factors greatly amplify each other. So it is vital for risk managers to strengthen operational resilience and crisis management frameworks and combine them with smart diversification and hedging.

Any crisis always brings new opportunities. Some 14 years ago, risk managers learned tough lessons on how to navigate extreme global financial shocks. Dealing with today's toxic mix of events, industry leaders have the chance to bring their management frameworks to a new level — and it is a chance that they will have to take if they are to mitigate the tail risks of what appears to be a perfect storm.

Press Corner

Cyber attackers: if you can't stop them, disrupt them

Best defence can be identifying vulnerabilities and blocking digital assault pathways

© Efi Chalikopoulou

Hannah Murphy in San Francisco JUNE 1 2022

For decades, companies have bolstered their cyber defences in a bid to thwart intruders. But while this work will always continue, firms are increasingly confronting the reality that it takes only a small slip-up, or an unnoticed flaw, for hackers to be able to get inside their systems. And then what?

So, in a shake-up of approach, many businesses are now focusing on how to mitigate cyber attacks — on the assumption that a breach is inevitable.

Some firms create internal "red teams" to probe their own systems for weaknesses, but Padraic O'Reilly, chief product officer and co-founder of cyber security risk group CyberSaint, says companies should do more "proactive or mitigative remediation".

"You will be planning for budget cycles, and looking at risk and making risk-informed decisions, instead of just putting out fires."

What can go wrong?

People	Systems	Processes	External Events
Fraud, collusion and other criminal activities	IT problems (hardware, software, hacking, viruses)	Execution, registration, settlement and documentation errors	Criminal activities (theft, vandalism, terrorism)
Violation of internal or external rules (secrecy, ethical rules, the law)	Software bugs	Errors in models, methodologies and mark to market	Political and military events (war, coup d'etat, internacional sanctions)
Incompetence or negligence	Unauthorized access to information	Compliance errors (accounting, taxation, reporting)	Changes in the political, legal, regulatory and tax environment
Loss of important employees (illness, problems retaining staff)	Unavailable and questionable integrity of data	Inadequate procedures, bad business practices	Natural events (fire, flood, earthquakes)
Violations of system securities	Utility outages (power, telecoms)	Inadequate definition and attribution of responsibilities	Operational failure at suppliers and outsourcers

Operational Risk: a special kind of risk

Financial Risks	Operational Risk
Consciously and willingly faced	Unavoidable
Speculative risks, implying profits or losses	Pure risks, implying losses only
Consistent with an increasing relationship between risk and expected return	Not consistent with an increasing relationship between risk and expected return
Easy to identify and understand	Difficult to identify and understand
Comparatively easy to measure and quantify	Difficult to measure and quantify
Large availability of hedging instruments	Lack of effective hedging instruments
Comparatively easy to price and transfer	Difficult to price and transfer

Measuring Operational Risk

Phase	Activity	Outcome
1	Identification of risk factors	Risk Map
2	Estimating exposures to risk factors	Exposure Indicator (EI)
3	Estimating probability of occurrence of risky events (frequency)	Probability of Event (PE)
4	Estimating loss in case of event (severity)	Loss Given Event (LGE ou LGER)
5	Estimating expected loss	Expected Loss EL = EI x PE x LGER
6	Estimating unexpected loss	Unexpected Loss (UL)
7	Estimating OR capital at risk	Capital at Risk (CaR)

This table is taken, with adaptation, from Resti and Sironi.

Measuring Operational Risk

Phase	Activity	Outcome
1	**Identification of risk factors**	**Risk Map**
2	**Estimating exposures to risk factors**	**Exposure Indicator (EI)**
3	Estimating probability of occurrence of risky events (frequency)	Probability of Event (PE)
4	Estimating loss in case of event (severity)	Loss Given Event (LGE ou LGER)
5	Estimating expected loss	Expected Loss EL = EI x PE x LGER
6	Estimating unexpected loss	Unexpected Loss (UL)
7	Estimating OR capital at risk	Capital at Risk (CaR)

This table is taken, with adaptation, from Resti and Sironi.

Risk Map

Business Unit	Business Line	Risk	Event	EI
Retail Bank	Deposits	People	Software failure	Fees
Investment Banking	Cards	Systems	Hardware failure	Fees
Brokerage	Insurance	Processes	Communication Failure	Provisions
		External Events		

Measuring Operational Risk

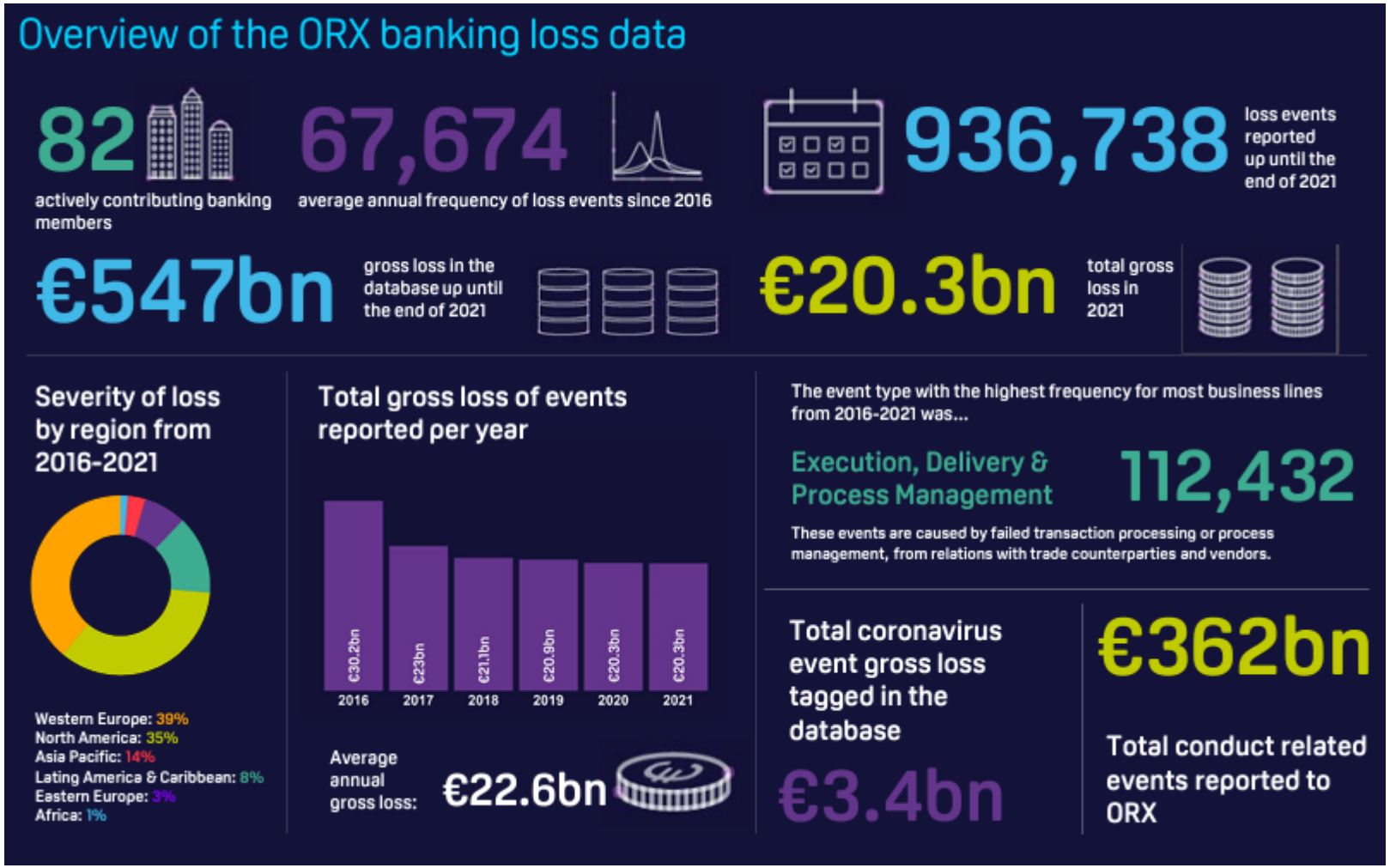
Phase	Activity	Outcome
1	Identification of risk factors	Risk Map
2	Estimating exposures to risk factors	Exposure Indicator (EI)
3	**Estimating probability of occurrence of risky events (frequency)**	**Probability of Event (PE)**
4	**Estimating loss in case of event (severity)**	**Loss Given Event (LGE ou LGER)**
5	**Estimating expected loss**	**Expected Loss EL = EI x PE x LGER**
6	Estimating unexpected loss	Unexpected Loss (UL)
7	Estimating OR capital at risk	Capital at Risk (CaR)

This table is taken, with adaptation, from Resti and Sironi.

Tolerance Risk Matrix

Severity ↓	Less than once every 5 years	Once per year to once every 5 years	Once per quarter to once a year	Once per month to once per quarter	More than once per month
above 50M€	Medium	High	High	Catastrophic	Catastrophic
1M€ to 50M€	Low	Medium	High	High	Catastrophic
100.000€ to 1M€	Low	Low	Medium	High	High
10.000€ to 100.000€	Insignificant	Low	Low	Medium	High
Below 10.000€	Insignificant	Insignificant	Low	Low	Medium
Frequency →					

Operational Risk – Loss Data



Measuring Operational Risk

Phase	Activity	Outcome
1	Identification of risk factors	Risk Map
2	Estimating exposures to risk factors	Exposure Indicator (EI)
3	Estimating probability of occurrence of risky events (frequency)	Probability of Event (PE)
4	Estimating loss in case of event (severity)	Loss Given Event (LGE ou LGER)
5	Estimating expected loss	Expected Loss EL = EI x PE x LGER
6	**Estimating unexpected loss**	**Unexpected Loss (UL)**
7	**Estimating OR capital at risk**	**Capital at Risk (CaR)**

This table is taken, with adaptation, from Resti and Sironi.

Expected and Unexpected Losses

For a similar expected losses, we can have very different unexpected losses:

Business Units	Unit A	Unit B
PE %	0,2%	10%
LGE (M€)	100	2
EL = PE x LGE (M€)	0,2	0,2

In this case, the unexpected loss of A is much higher than the unexpected loss of B.

Nerd's corner…

- If you don't have a better model, use the binomial distribution: an event will occur or not.
- So we can compute the average and the standard deviation.
- In our previous example, the average is 0,2 M€ in both cases, but standard deviations are 4,47 M€ for A and 0,60 M€ for B.
- This example assumes a non stochastic loss, which is not realistic. Knowing the loss variance, the new standard deviation is:

$$\sigma = \sqrt{PE \times (1 - PE)(LGE)^2 + PE \times \sigma_{LGE}^2}$$

Event	Prob.	Loss
occurrence	**PE**	**LGE**
no occurrence	**1 - PE**	**0**

$$EL = PE \times LGE$$

$$\sigma = \sqrt{PE \times (1 - PE) \times (LGE)^2}$$

Computing UL and CAR

- Assume a probability distribution for the expected loss;
- Assume a confidence interval;
- Compute the multiplier (number of standard deviations from the mean) for the distribution and the confidence level;
- Unexpected Loss (UL) is the product of the multiplier and the standard deviation;
- CaR is Unexpected Loss (UL) plus Expected Loss (EL).

(This is an exception to the general concept of CaR = UL, as banks do not provision the EL for operational risk)

- More advance methods might use different distributions for each business unit (or coppula methods), or different distributions for PE and LGE, or use Monte Carlo simulation.

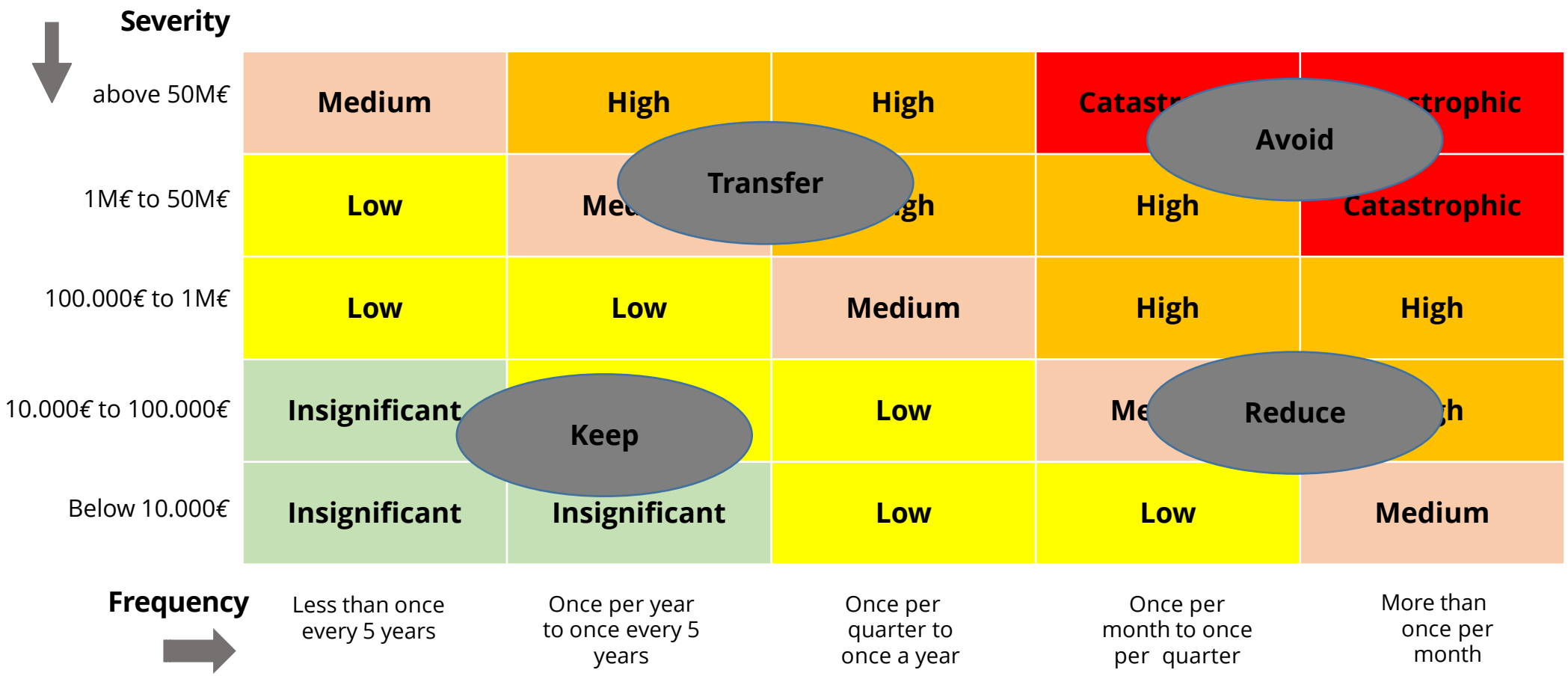
Managing Operational Risk

- When we hear about operational risk, most often the concern seems to be the computation of regulatory capital.

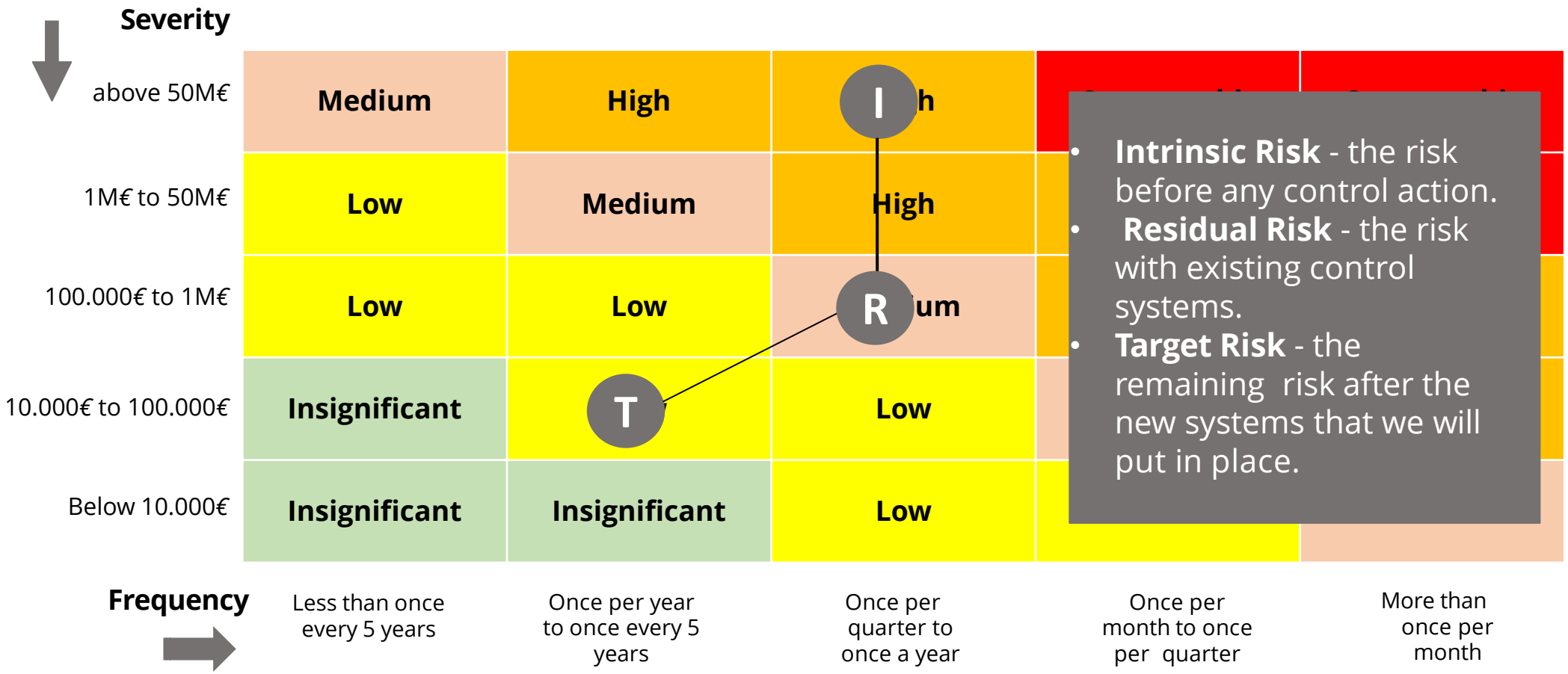
- However, we should also manage the risk.

- The most relevant contribution from Basel II, in terms of Operational Risk, is the awareness of the risk, and the opportunity to start managing it.

Strategy for the Risk Matrix



Managing the Risk Matrix



- **Intrinsic Risk** - the risk before any control action.
- **Residual Risk** - the risk with existing control systems.
- **Target Risk** - the remaining risk after the new systems that we will put in place.

Operational Risk – Data Management – an example

- We need to build a data repository for each event occurrence.
- And we need a workflow to deal with each occurrence:
  - Whenever an event occurs, we need to open an incident (v.g. time deposit interests are miscalculated, client complaint);
  - the incident is classified according to the risk map and the risk manager is alerted;
  - the manager must check what happened (deposit features in the system are different from the ones agreed with client; the interest code was wrongly input by operator; the system miscalculates interests in leap years; the client is confused and everything is OK);
  - finally, the incident is closed by the process owner, declaring “non event”, “event with loss” or “event without loss”. The loss is also registered.
- If appropriate, the process owner must also write a recommendation on how to avoid future occurrences of the same event (double check on manual inputs, bug fix).

Operational Risk – a dynamic methodology

- The relevant risks may change in time (new lines of business, technology, new threats,…);
- Accumulating experience, all parameters can be fine tuned;
- New control systems change PE and LGE, call for Target Risk revision and new plans;
- All the OR management system should be audited, most often by central banks.

Operational Risk – an integrated system

The Board

Promotes a passion for quality, fights for informed and responsible risk taking, assigning authority to managers. Keep the appropriate core capital to cover unexpected losses (pillar I).

Bank Managers

Identify, track and mitigate the risks, and perform a periodic audit of the system;

Supervisors

Guarantee that all banks have in place appropriate OR management systems, and perform regular audits (pillar II);

Market

Demand an appropriate reporting for them to be able to assess the quality of the system and the level of risk taking (pillar III).

Operational Risk – supervisory requirements

- The January 2001 consultation of the Basel II Accord, for the first time, introduced operational risk as part of risk-weighted assets (RWAs).
    - need to calculate minimum capital requirements for operational risk.

- Three methods were introduced:
    - The basic indicator approach (BIA).
    - The standardised approach (TSA).
    - The internal measurement approach (IMA).

Operational Risk – supervisory requirements

Basic indicator approach

- Average of last 3 years of the Gross Income (GI) x 15%

corporate finance
trading & sales
retail banking
commercial banking
payment & settlement
agency services
asset management
retail brokerage.

Standardised approach

- Approach by business lines defined by the regulator
- A single exposure indicator: the GI of each business line (last 3 yrs average)
- A weighting factor by business line reflects the risk related to the activity

Advanced measurement approach (AMA)

- The most sophisticated and complex option under Basel II.
- Allows a bank to calculate its regulatory capital charge using internal models, based on internal risk variables and profiles, and not on exposure proxies such as gross income.
- This is the only risk-sensitive approach for operational risk allowed and described in Basel II.

Capital requirements: AMA – the future?

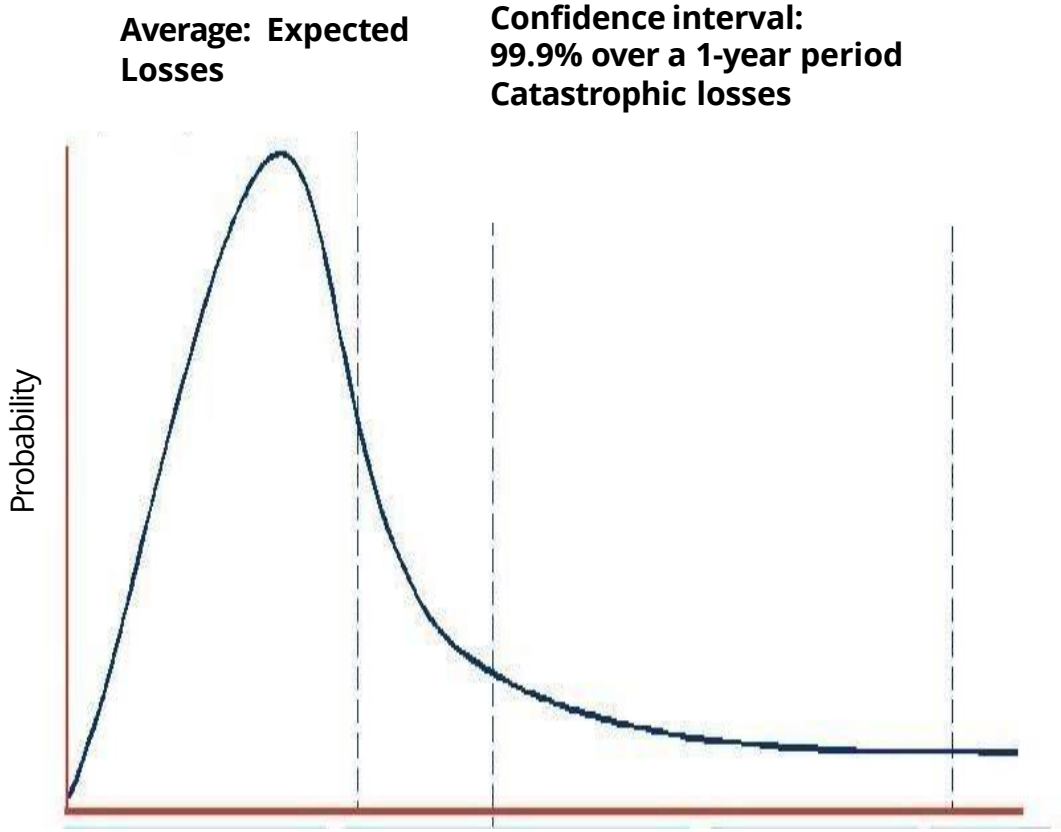
- The capital requirement is calculated using an internal model developed by the bank under qualitative and quantitative constraints:

$$K_{AMA} = EL + UL$$

- If the bank demonstrates that is adequately capturing EL in its internal business practices, the base to capital requirements can be UL alone.

- Few details are given on the calculation methods used by this model.

- The effective use of an internal model is subject to the prior approval by the regulator.



Capital requirements: AMA – the future?

AMA has presented some practical problems…

- Difficulty in modelling extreme events is related with the absence of data for rare events.
- Insufficient data on extreme events makes it necessary to consider external data and experts' opinions.

- However, the importance and value of advanced risk management practices and measurement cannot be overestimated: they play a critical role in protecting the bank's value!

Basel – A revised framework for operational risk

BANK FOR INTERNATIONAL SETTLEMENTS

- In December 2017, the Basel Committee on Banking Supervision introduced the new standardised approach for calculating operational risk capital charge, which replaces all operational risk approaches under Basel II.

Components of the standardised approach

- Under the new standardised approach, operational risk capital is calculated as follows:

Source: BIS

Basel – A revised framework for operational risk

BANK FOR INTERNATIONAL SETTLEMENTS

The business indicator component (BIC)

- The BIC corresponds to a progressive measure of income that increases with a bank's size.
- It serves as the baseline capital requirement and is calculated by multiplying the Business Indicator (BI) by marginal coefficients.
- The BI is a financial statement-based proxy for operational risk consisting of three elements, each calculated as the average over three years:

    1. the interest, leases and dividend component;
    2. the services component;
    3. and the financial component.

- Marginal coefficients are regulatory determined constants based on the size of the BI.

Basel – A revised framework for operational risk

BANK FOR INTERNATIONAL SETTLEMENTS

The internal loss multiplier (ILM)

- The ILM is a risk-sensitive component capturing a bank's internal operational losses.
- It serves as a scaling factor that adjusts the baseline capital requirement depending on the operational loss experience of the bank.
    - The inclusion of banks' own historical losses through the ILM indicator would either increase their capital requirement for operational risk in case the banks suffered large operational risk losses in the past (in this case ILM would be higher than 1) or decrease it if banks did not suffer such losses (in this case ILM would be lower than 1
- In calculating the LC, banks need to meet the requirements on loss data identification, collection and treatment.

Basel – A revised framework for operational risk

BANK FOR INTERNATIONAL SETTLEMENTS

Disclosure and implementation timeline

- All banks need to disclose each BI sub-item for each of the three years of the BI calculation window.
- Moreover, banks with BI exceeding EUR 1 billion, or that use internal loss data in the calculation of operational risk capital, need to disclose their annual loss data for each of the 10 years in the ILM calculation window.

Operational Risk @ European Union level

Banking Package 2021: new EU rules to strengthen banks' resilience and better prepare for the future

- **European Commission proposal on operational risk (2021 Oct.):** The single risk-sensitive standardised approach to be used by all banks, replacing all the existing standardised and internal model approaches for this risk.
    - aim: simplification of the framework and increase comparability

- The supervisory discretion introduced in the Basel III standards that allows supervisors to set ILM to 1 for all banks in their jurisdictions has been used and ILM has been set to 1.
    - disregard banks' own historical losses as a driver of the level of their capital requirement for operational risk.
    - While there is empirical evidence showing that banks experiencing greater operational risk losses historically are more likely to experience operational risk losses in the future, the events that have led to the largest operational losses are less amenable to prediction based on historical loss data than for other types of risks.

Source: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_5401

Banking

Ana Lacerda

Fall Semester 2024

Course: Banking [2206]