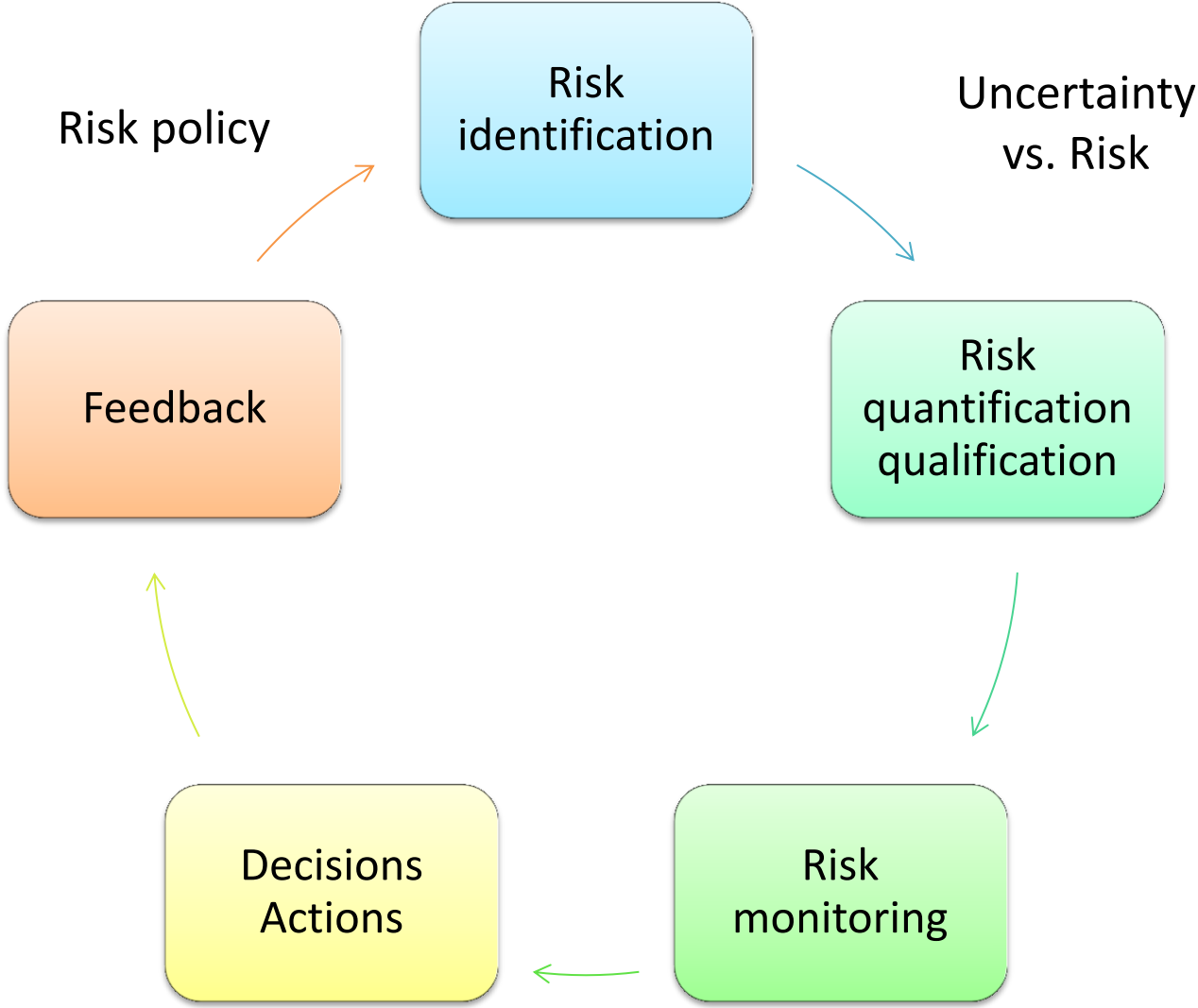


Risk Management and Governance

OpRisk, LiqRisk & Governance

Prof. Hugues Pirotte

Risk Management Process



Keep focus on the objective!



TELL US AGAIN WHY WE NEED THREE HUNDRED HORSEPOWER TO GET GROCERIES.

Liquidity can hide the truth...



Operational Risk

(based on various sources including Ariane Chapelle slides, practical examples, etc...)

Operational Risk

- One more type of risk to be assessed for regulatory purposes (for banks)
 - » People (errors, fraude)
 - » Systems (any physical incident, etc...)
 - » Procedures (lack, ineffective implementation or execution, bad delivery)

- Operational risk, in a broader sense, covers also the implementation of the good risk management policy
 - » Risk management framework
 - 1) Identification & Assessment
 - 2) Managerial decisions & actions (mitigation, etc...)
 - 3) Monitoring
 - 4) Feedback on the framework

Aims of Financial Regulation

- Regulation - Three policy objectives
 - » To ensure the solvency and soundness of all financial intermediaries
 - » To provide depositors protection from undue risks (failure, fraud, opportunistic behaviour)
 - » To promote the efficient and competitive performance of financial institutions
- Supervision
 - » Implementation of regulation
- Internal controls
 - » Undertaken by the owners of a financial institution to prevent or detect fraudulent behaviour

Risks in Financial Intermediation

- Included in the mainstream regulation (current Basle II)
 - » Credit risk (70%): counterpart risk
 - » Market risk (18%): interest rate risk & liquidity risk
 - » Operational risk (12%): fraud - errors - IT and physical damage to assets
- Other risks
 - » Transfer risk (often included in credit)
 - » Legal risk (often included in operational risk)
 - » Business risk (strategic risk)
 - » Reputation risk (as a result of bad operational risk management)

Specificities of Operational Risk

- The Specific Nature of Operational Risk
 - » Embedded risk
 - ✓ Not a transaction-risk but a risk embedded in processes, people and systems and due to external events.
 - » Inherent risk
 - ✓ A large part of operational risk is inherent to the business in which we are engaging and inherent to management processes.
 - » Hidden risk
 - ✓ The costs due to OR are difficult to trace or anticipate since most are hidden in the accounting framework.
 - ✓ Leads to underestimation of the risk (e.g. information security).
 - » Unstable risk
 - ✓ Not linearly linked to the size of the activities. Small activities can be very risky, and vice versa.
 - ✓ OR can be very unstable and grow exponentially in a short period.
 - » Reputation risk
 - ✓ A second order risk, leading to additional damage in the form of damage to reputation.

Basle Reform for Operational Risk

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events.

Categories of OR events

- **Execution, Delivery & Process Management** (processing error, information transfer, data coding,...)
- **Clients, Products & Business Practices** (clients misinformation, complaints and discounts due to errors, products misspecification...)
- **Internal fraud** (thefts and frauds by employees)
- **External fraud** (hold-up, thefts,..)
- **Employment practices & workplace safety** (contract termination, disputes with employees...)
- **Damage to physical assets**
- **Business disruption & system failures** (IT break-down, hacking...)

Categorization of Business Lines

- Corporate finance
- Trading and sales
- Retail banking
- Commercial banking
- Payment and settlement
- Agency services
- Asset management
- Retail brokerage

Basle Reform for Operational Risk

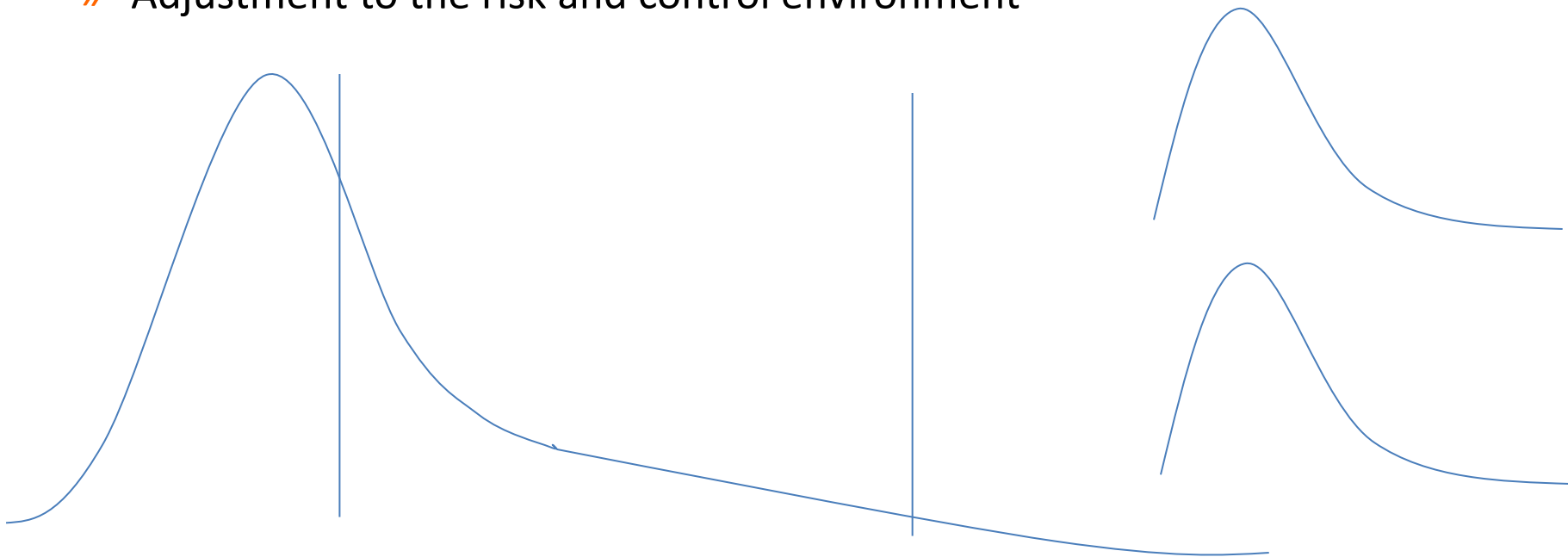
- Regulatory Capital for OR introduced for the first time
- Rule of thumb : OR capital = 12% of minimum capital requirement
- 1) Basic indicator approach (BI):
 - » OR capital function of gross income (15%)
 - » Gross income = interest margin + fees + other revenues
 - » Only accessible to local banks
- 2) Standardised approach (β)
 - » OR capital function of gross income per business line
 - » Beta factor between 12% and 18% of gross income, estimated via QIS on a sample of 29 institutions.

and an advanced approach...

- 3) Advanced Measurement Approach (AMA) in Basle II:
- » Banks are free to model their OR capital themselves
 - » Strongly recommended for internationally active banks
 - » Floor capital at 75% (so far) of the capital level under the Standardised Approach, and 9% of total regulatory capital
 - » Submitted to quantitative and qualitative standards, such as:
 - ✓ incident reporting history of 5 years, minimum 3 years;
 - ✓ mapping of risks and losses to regulatory categories
 - ✓ independent ORM function;
 - ✓ implication of the senior management;
 - ✓ written policies and procedures;
 - ✓ active day-to-day OR management.

Fours Components of AMA

- In order to be AMA compliant, financial institutions should demonstrate:
 - » Internal loss data collection
 - » External loss data collection and use in modelling economic capital
 - » Scenario Analysis
 - » Adjustment to the risk and control environment



Op Risk – Many competencies

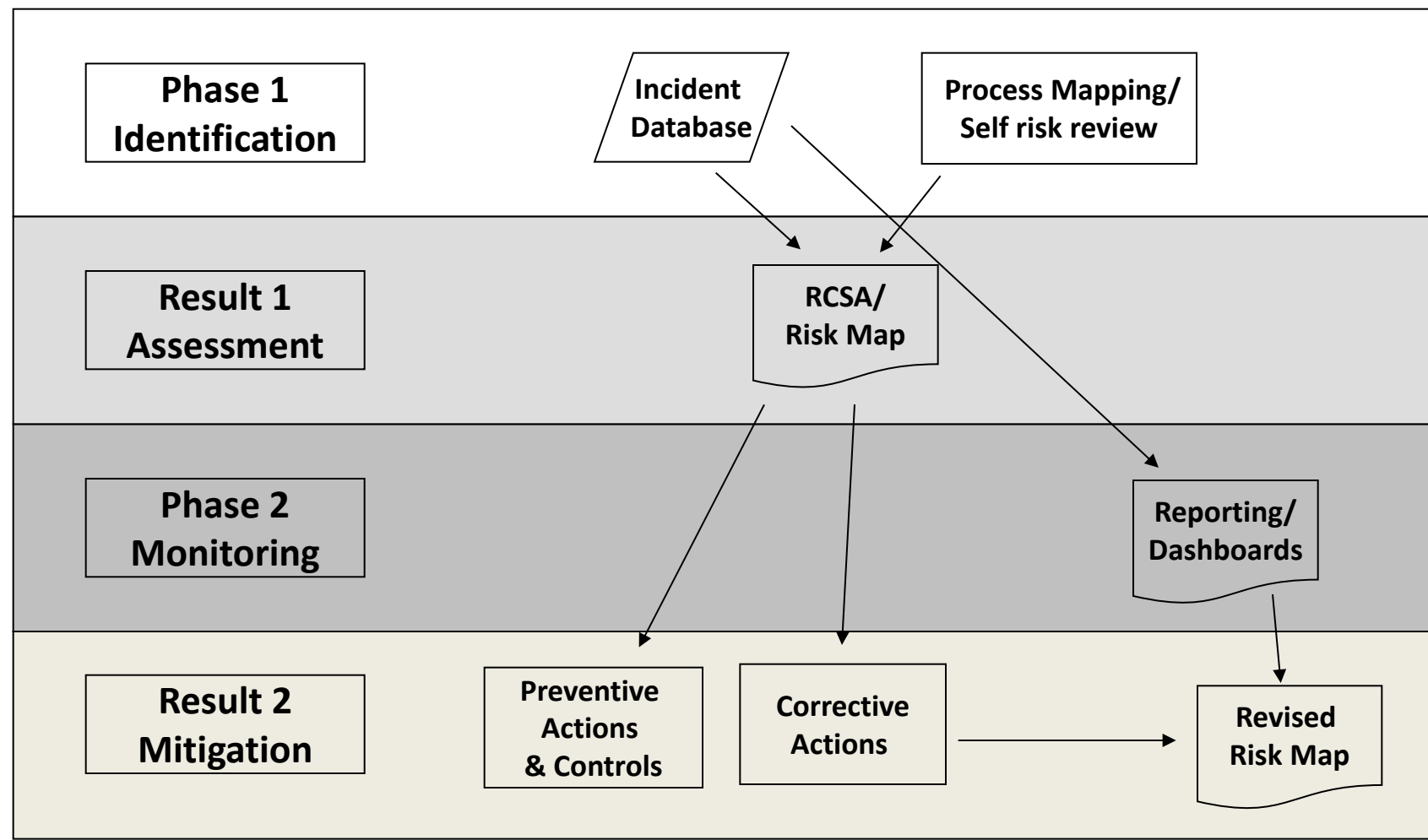
Underlying causes of operational losses : processes - people - systems - or external events.

Legal risk included , strategic and reputation risk excluded.

Appropriate manager per category of operational event :

- ✓ Execution, Delivery & Process Management : ORM
- ✓ Clients, Product & Business Practices : ORM
- ✓ Internal fraud : Inspection / ORM
- ✓ External fraud : Inspection (Compliance)
- ✓ Employment practices & workplace safety : Security
- ✓ Damage to physical assets : Security
- ✓ Business disruption & system failures : IT / Security

A Simple ORM Framework in practice



Incident Reporting

- Important tool to:
 - » Raise risk awareness
 - » Assess the risk, when materialised
 - » Prioritise action plans

- It is a:
 - » First assessment of the losses
 - » First instrument for a Risk Map, at least retrospective

Risk Identification - Incident Reporting

- ✓ Fields to include per event :
 1. Dates: discovery – reporting - closing
 2. Event localisation : BU, department, service
 3. Event type : codification of Basle categories
 4. Business line : codification of Basle categories
 5. Comment : nature of the event
 6. Gross Loss amount
 7. Recovery amount : via insurance / other
 8. Actions taken : preventive / corrective
 9. Reporter coordinates

	ID	BU	Branch	Gross Loss	Recovery	E type	...
Event 1							
Event 2							
...							

Loss Data Analysis

- Two main types of events:
 - » Large Risks, to be known and reported immediately
 - ✓ Require a more detailed reporting
 - ✓ Lead to action plan
 - ✓ And to a follow-up of the actions
 - » Small, frequent risks
 - ✓ Recurrent, small, similar events
 - ✓ May signal a breach in control -> immediate action needed
 - ✓ Could be inherent to the activity -> to be included in pricing
 - ✓ Useful for statistics and distribution modeling

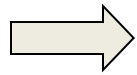
Loss Reporting

- Dashboards: the simpler the better
- Comparative
 - » Through time: trend analysis -> wrong signal if rising
 - » Across departments: e.g. comparisons of different commercial units, and comparison to the mean
 - » Adapted to the type of activity

Example

UNIT	TOTAL ALL				
	Number	Amount	Average	Loss/Income %	TOP 5 amounts
Q 1					1.
Q 2					2.
Q 3					3.
Q 4					4.
					5.
PER TYPE					
<i>Type x</i>					
	Number	Amount	Average	Loss/Income %	TOP 5 amounts
Q 1					1.
Q 2					2.
Q 3					3.
Q 4					4.
					5.

Paradox of incident data collection



Crucial data choice in the capital determination



Paradox of the incident data collection :

- Data collection is mandatory,
- But external data essentially drive the capital amount.

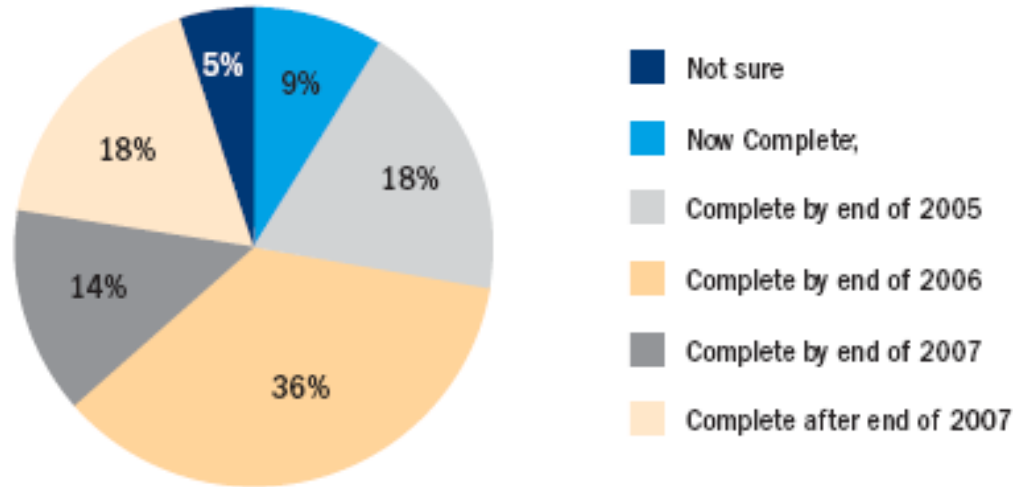


Data collection needed for active ORM reasons.

Data collection – Where do we stand e.g. in 2005?

- Loss data collection under way:

Figure 17: Status of operational risk quantification among CEE survey's respondents collecting loss data



Source: Ernst&Young, “Basel II Survey, Central and Eastern Europe”, June 2005.

Process Mapping

- Definition

- » A flowchart is a graphical representation of a process.
- » It represents the entire process from start to finish, showing inputs, pathways and circuits, action or decision points, and ultimately, completion.
- » It can serve as a tool for facilitating optimization of workflow highlight risk and control needs.

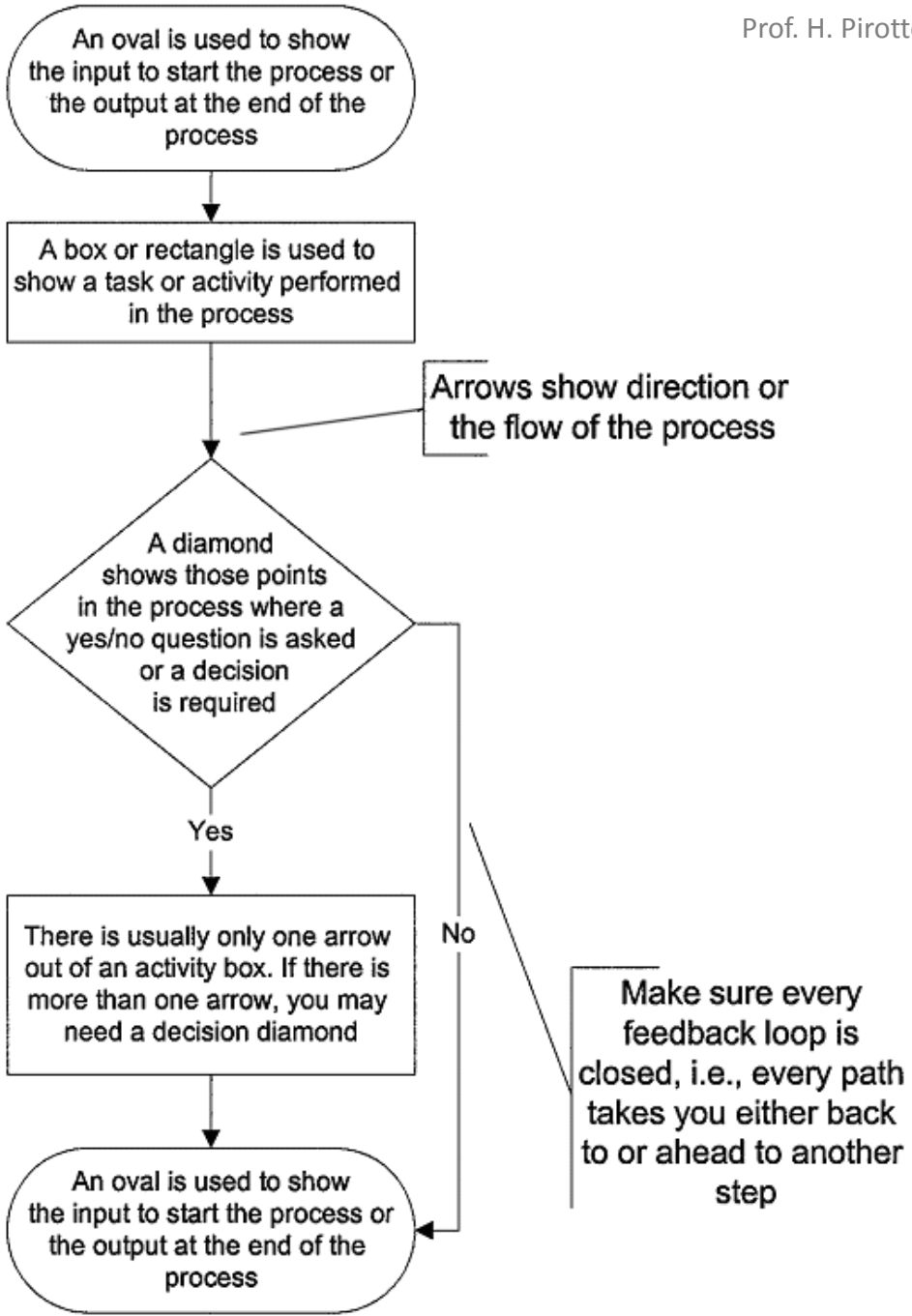
Process Mapping - Steps

- Step 1: Determine the Boundaries
 - » Where does a process begin?
 - » Where does a process end?
- Step 2: List the Steps
 - » Use a verb to start the task description.
 - » The flowchart can detail every finite action and decision point.
- Step 3: Sequence the Steps
 - » Use post-it notes so you can move tasks.
 - » Do not draw arrows until later.

Process Mapping - Symbols

- Step 4: Draw Appropriate Symbols
 - » Ovals show input to start the process or output at the end of the process.
 - » Boxes or rectangles show task or activity performed in the process.
 - » Arrows show process direction flow.
 - » Diamonds show points in the process where a yes/no questions are asked or a decision is required.
 - » Usually there is only one arrow out of an activity box. If there is more than one arrow, you may need a decision diamond.
 - » If there are feedback arrows, make sure feedback loop is closed; i.e. it should take you back to the input box.

Example Flowchart



Source: Iowa State University

Process Mapping – Risk Identification

- Step 5: Check for Completeness
 - » Include pertinent chart information, using title and date
 - » Review all tasks

- Step 6: Finalize the Flowchart
 - » Identify potential sources of operational risk
 - » Ask if this process is being run the way it should be
 - » Ask if the controls are where there should be, appropriate and sufficient to limit risks.

Risk & Control Self Assessment (RCSA)

- Sources of RCSA
 - » Incident reporting analysis
 - » Orientation questionnaires with selected people from the department.
 - » Check list from the key risks library
 - » Process mapping
 - » Prioritization list with the line management

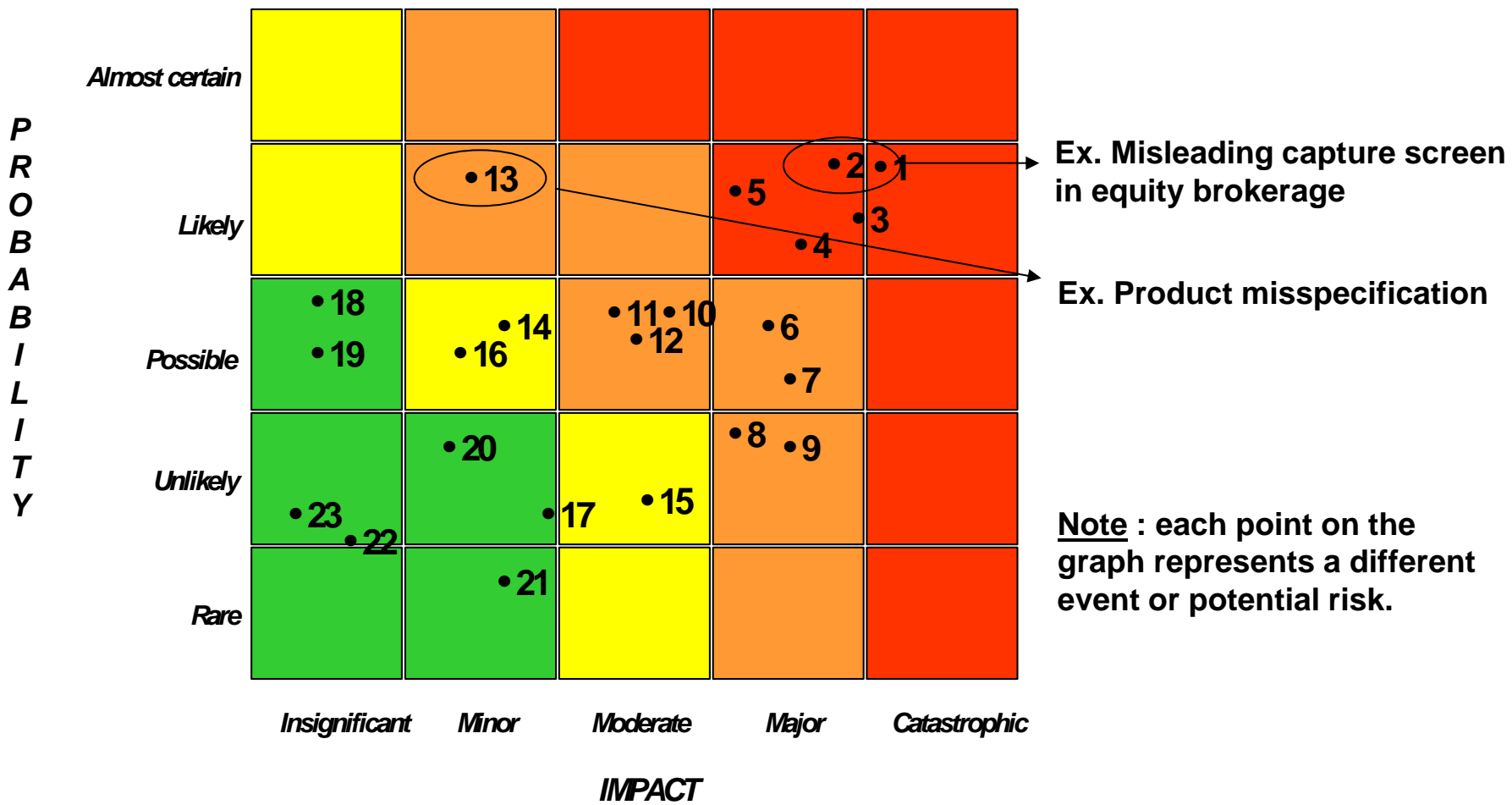
Risk & Control Self Assessment (RCSA)

- RCSA performed by local management, with the support of ORM
 - » Top management: identification of key risk areas
 - » -> RCSA processes for all key businesses and functions
 - » Apply & document the RCSA process
 - » Progress-tracking of mitigating actions
 - » Line management is responsible for the output

RCSA

Assessment : Impact / Probability Matrix

Based on a *risk analysis report* which reflects all (residual) risks and controls.



Deliverables of a RCSA exercise

- An estimate of the expected losses
 - » the average loss if the risk event occurs
 - » the average yearly frequency of the risk event
- An estimate of stress shortfalls
 - » Maximum financial impact that could occur in the future and likelihood of occurrence in the year to come:
 - ✓ the maximum loss
 - ✓ its related yearly frequency

Types of Impacts




- Six types of impacts following an event:
 - » Immediate Financial Impact
 - » Significant Non-Financial Impact :
 - ✓ Regulatory
 - ✓ Person-days lost
 - ✓ Forgone revenue
 - ✓ Reputation
 - ✓ Work Environment
 - ✓ Human

KPIs – KRIs

- Risks indicators
 - » Early warning devices
 - » Specific to each activity
 - » Identified through check lists or risks self assessments and expert opinions
- Performance indicators
 - » Materialise the symptoms of the risks
 - » Dependent of the strategic priorities of the business
 - » Need heavy data collection
 - » Requires performant information collection system
- Analysis and thresholds
 - » To set according to the priorities of the business

KRIs & KPIs - Examples

- ✓ People: turn-over, temporary staff, overtime, client complaints, absenteeism
- ✓ Processing: outstanding confirmations, (status/duration of) reconciliation; failed & overdue settlements; claims & complaints; manual bookings; reversals
- ✓ Accounting: volumes & lead-times suspense-accounts; reversals;
- ✓ Systems: logs of downtimes; hacking-attempts; project-planning-overruns

Risk Category	KRI	Measures Required*	Tolerance Levels	Actual Score	Indicator	Management Action
Transaction Recording/ Processing	Front/Back Office reconciling items	No >1 day, Value				
Transaction Recording/ Processing	Net marginal cost of interest charging	Value				
Trade Settlement	Trade Fails	% of month's trades, duration of total fails				

KRI - Challenges

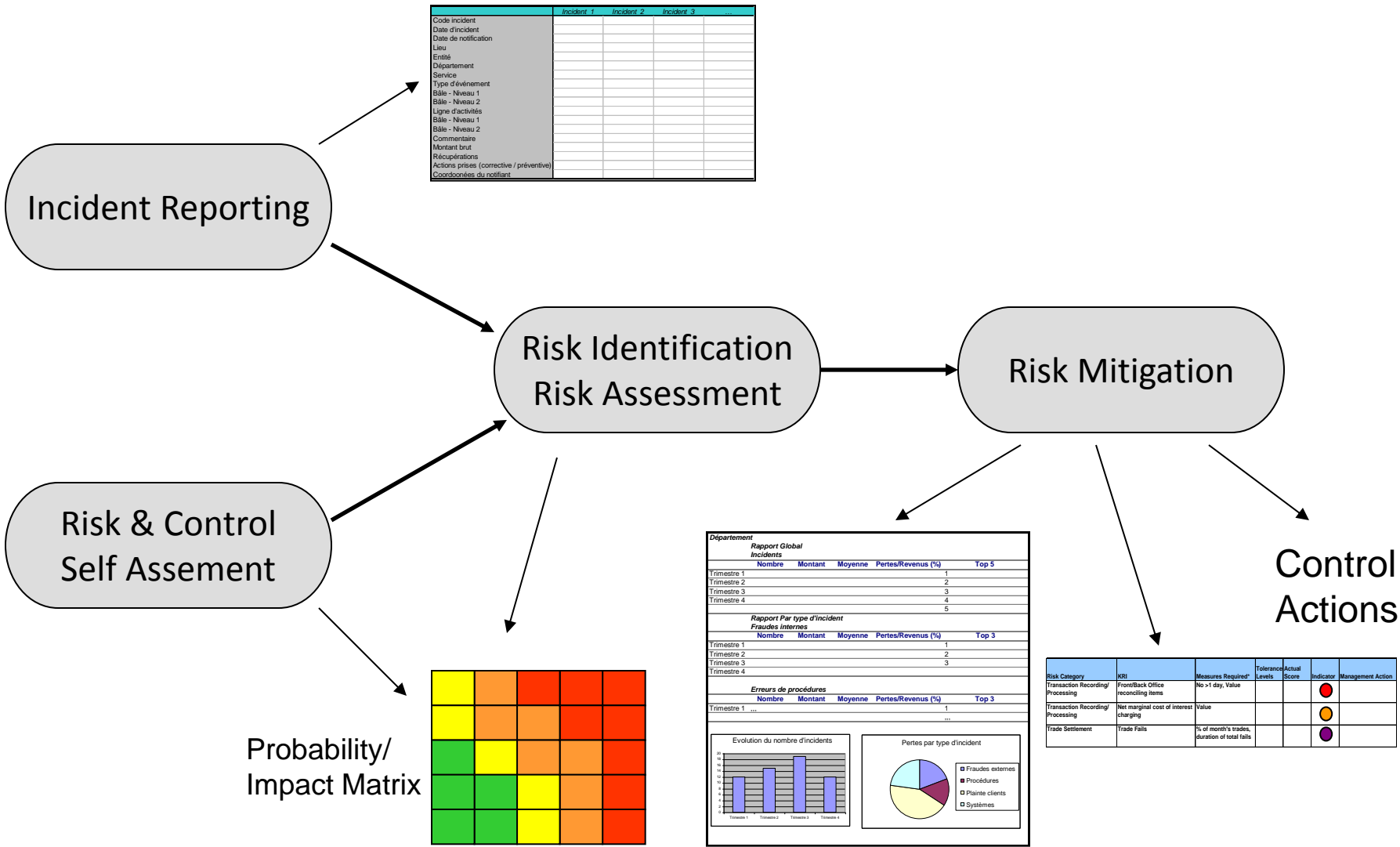
- KRIs do not always track risk well:
 - » Mainly because they defined at a too high level
 - » KRI to be mapped a process level
 - » A single indicator can cover several risks

7 Rules of efficient KRI

1. Incorporating Risk Drivers
 - » Addresses risks, not events
2. Quantifiable: €, %, #
 - » Measures the risk, to manage it
3. Time series tracked against standards or limits
 - » Limits are linked to risk appetite and strategic importance of the risk
4. Tied to objectives, risk owners and standard risk categories
 - » Classify KRI by types of risks addressed, or by businesses incurring the risk (risk owners)
5. Linked to preventive or corrective controls, supporting management decisions and action
6. Timely and cost effective
7. Simplifying risk

Source: James Lam & Associates, 2006.

Operational Risk- Framework and Tools



	Incident 1	Incident 2	Incident 3
Code incident			
Date d'incident			
Date de notification			
Lieu			
Entité			
Département			
Service			
Type d'évènement			
Bille - Niveau 1			
Bille - Niveau 2			
Ligne d'activités			
Bille - Niveau 1			
Bille - Niveau 2			
Commentaire			
Montant brut			
Récupérations			
Actions prises (corrective / préventive)			
Coordonnées du notifiant			

Département					
Rapport Global Incidents					
	Nombre	Montant	Moyenne	Pertes/Revenus (%)	Top 5
Trimestre 1					1
Trimestre 2					2
Trimestre 3					3
Trimestre 4					4
					5
Rapport Par type d'incident					
Fraudes Internes					
	Nombre	Montant	Moyenne	Pertes/Revenus (%)	Top 3
Trimestre 1					1
Trimestre 2					2
Trimestre 3					3
Trimestre 4					
Erreurs de procédures					
	Nombre	Montant	Moyenne	Pertes/Revenus (%)	Top 3
Trimestre 1					1
Trimestre 2					
Trimestre 3					
Trimestre 4					

Risk Category	KRI	Measures Required	Tolerance Levels	Actual Score	Indicator	Management Action
Transaction Recording/Processing	Front/Back Office recording items	No >1 day, Value			Red Circle	
Transaction Recording/Processing	Net marginal cost of interest charging	Value			Yellow Circle	
Trade Settlement	Trade Fails	% of month's trades, duration of total fails			Purple Circle	

Liquidity risk

[based on Hull and own notes]

Measuring liquidity in transactions...

Cost of liquidation in normal markets...

$$\text{Proportional Bid-offer spread} = \frac{\text{Offer price} - \text{Bid price}}{\text{Mid-market price}}$$

Cost of liquidation in normal markets

$$\sum_{i=1}^n \frac{1}{2} s_i \alpha_i$$

where n is the number of positions, α_i is the position in the i th instrument, and s_i is the proportional bid-offer spread for the i th instrument

And in stressed markets...

$$\sum_{i=1}^n \frac{1}{2} (\mu_i + \lambda \sigma_i) \alpha_i$$

where μ_i and σ_i are the mean and standard deviation of the spread and λ gives the required confidence level

Liquidity adjusted VaR

$$\text{Liquidity-adjusted VaR} = \text{VaR} + \sum_{i=1}^n \frac{1}{2} s_i \alpha_i$$

$$\text{Liquidity-adjusted stressed VaR} = \text{VaR} + \sum_{i=1}^n \frac{1}{2} (\mu_i + \lambda \sigma_i) \alpha_i$$

Unwinding a Position Optimally (page 390)

- Suppose dollar bid-offer spread as a function of units traded is $p(q)$
- Suppose standard deviation of mid-market price changes per day is σ
- Suppose that q_i is amount traded on day i and x_i is amount held on day i ($x_i = x_{i-1} - q_i$)
- Trader's objective might be to choose the q_i to minimize

$$\lambda \sqrt{\sum_{i=1}^n \sigma^2 x_i^2} + \sum_{i=1}^n \frac{1}{2} q_i p(q_i)$$

Example 19.3 (page 391)

- A trader wishes to unwind a position in 100 million units over 5 days
- $p(q) = a + be^{cq}$ with $a = 0.1$, $b = 0.05$, and $c = 0.03$
- $\sigma = 0.1$
- With 95% confidence level the amounts that should be traded on successive days is 48.9, 30.0, 14.1, 5.1, and 1.9

Liquidity Funding Risk

- Sources of liquidity
 - » Liquid assets
 - » Ability to liquidate trading positions
 - » Wholesale and retail deposits
 - » Lines of credit and the ability to borrow at short notice
 - » Securitization
 - » Central bank borrowing

Examples of Liquidity Funding Problems

- Northern Rock (Business Snapshot 19.1)
- Ashanti Goldfields (Business Snapshot 19.2)
- Metallgesellschaft (Business Snapshot 19.3)

Liquidity Black Holes

- A liquidity black hole occurs when most market participants want to take one side of the market and liquidity dries up
- Examples:
 - » Crash of 1987 (Business Snapshot 19.4, page 358)
 - » British Insurance Companies (Business Snapshot 3.1)
 - » LTCM (Business Snapshot 15.4)

Positive and Negative Feedback Trading

- A positive feedback trader buys after a price increase and sells after a price decrease
- A negative feedback trader buys after a price decrease and sells after a price increase
- Positive feedback trading can create or accentuate a black hole

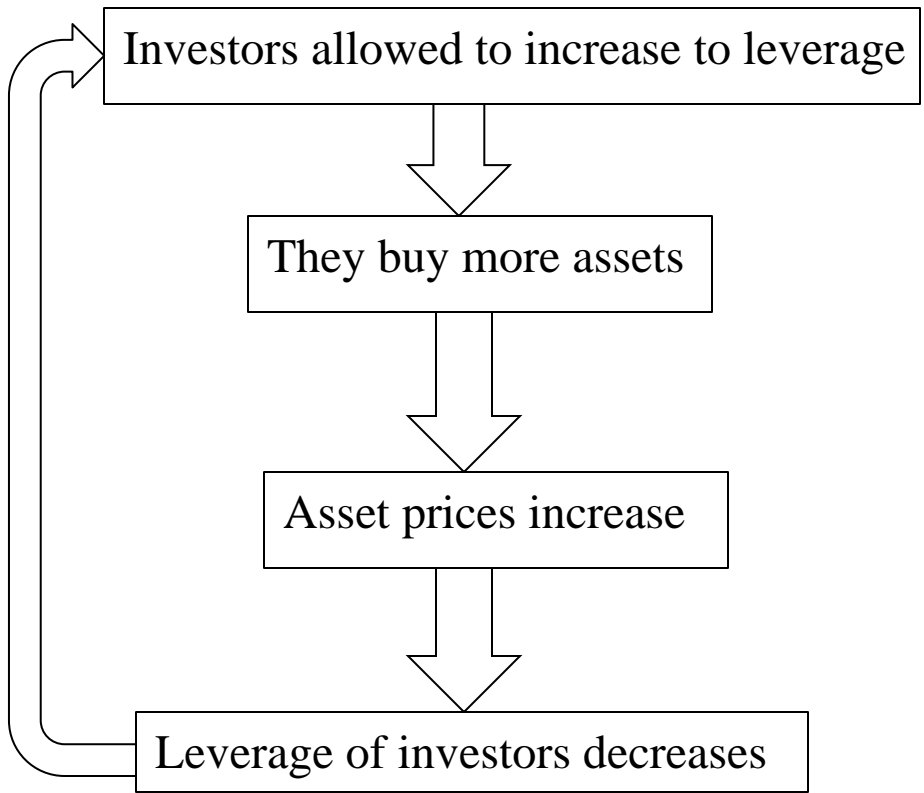
Reasons for Positive Feedback Trading

- Computer models incorporating stop-loss trading
- Dynamic hedging a short option position
- Creating a long option position synthetically
- Margin calls

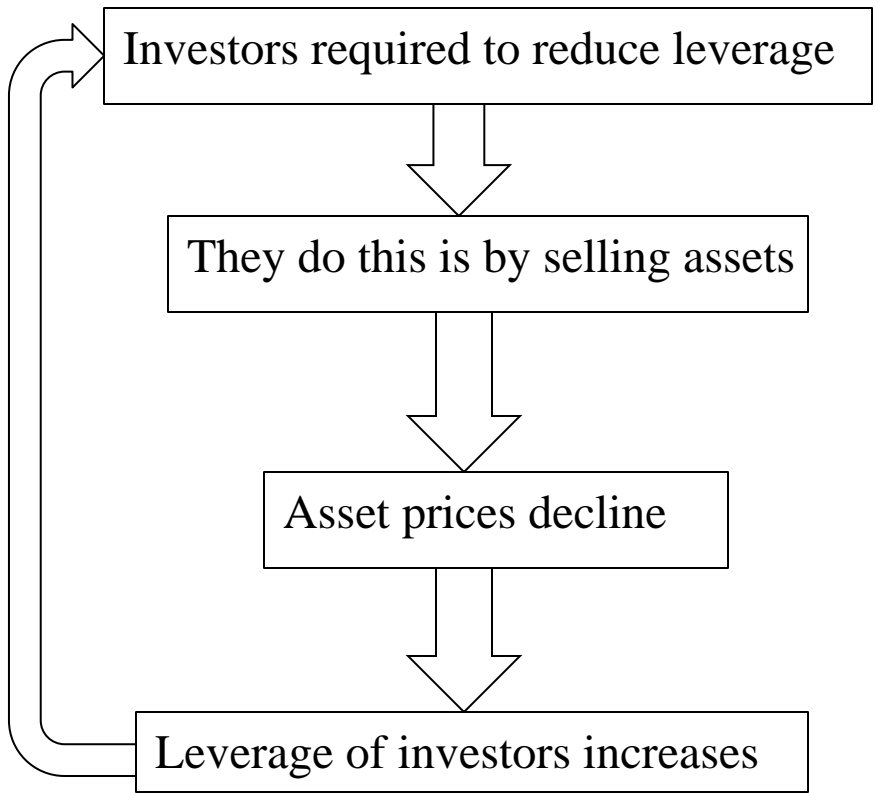
The Impact of Regulation

- If all financial institution were regulated in the same way, they would tend to react in the same way to market movements
- This has the potential to create a liquidity black hole

The Leveraging Cycle (Figure 19.2)



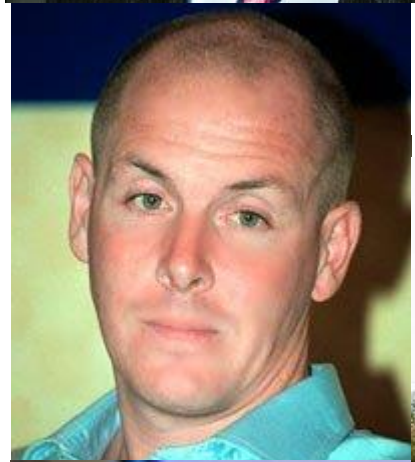
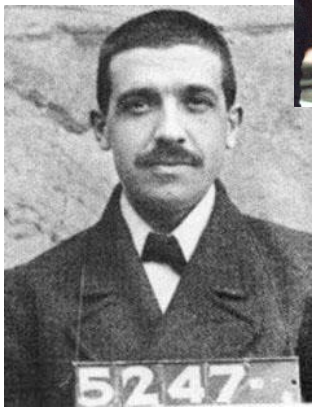
The Deleveraging Cycle (Figure 19.3)



Is Liquidity Improving?

- Spreads are narrowing
- But arguably the risks of liquidity black holes are now greater than they used to be
- We need more diversity in financial markets where different groups of investors are acting independently of each other

Risk Governance



SocGen – Rogue trading records

Facts (public)

- Soc Gen lost €4.9 bn in rogue trading activities in Jan 21-22-23, 2008.
- Rogue trader on equity futures built unauthorised, unhedged €50bn exposure from an arbitrage desk.
- Trader was performing unauthorised activities since 2005.
- Fictitious hedging transactions have been performed to make believe active bets were hedged.
- Fictitious transactions cancelled before settlement, or made with in-house counterparts with no margin calls.
- Both notional exposure and cancellation of deals supposedly undetected from control teams since 2005.
- Inquiries are underway.

Soc Gen – Control Failures

- So far, apparent control failures are:
 - » No check of notional amounts, only net positions
 - » No confirmation check for deals with in-house counterparties
 - » No red flag raised following several cancellations of deals from single trader
 - » No deep investigations following suspicion of large exposures built far beyond market authorised limits for a junior trader
 - » Lack of confidentiality of controls between front-office and middle-office (“calendar of controls” known)
 - » No / too few protection of logins and passwords of traders
 - » No red flags raised following suspicious behaviour (no holiday, no transfer of portfolio from trader)
 - »

Soc Gen - Questions

- Is the situation as it seems?
- Were managers unaware of breaching of trading limits?
- Did controls really fail?
 - » If not, why was the situation left as such?
 - » If yes, why so many failures?
- Could it happen again?
- Could it happen elsewhere?
- What is the course of action from now?

Some last advices...

Some advices for FIs

- Risk Limits
 - » Do not assume you can outguess the market
 - » Do not underestimate the benefits of diversification
 - » Carry out scenario analyses and stress tests
- Trading Room
 - » Separate the Front. Middle and Back Office
 - » Do not blindly trust models
 - » Be conservative in recognizing inception profits
 - » Do not sell clients inappropriate products
- Liquidity risk
 - » Beware when everyone is following the same trading strategy
 - » Do not finance long-term assets with short-term liabilities
 - » Market transparency is important

...and non-FIs

- Lessons
 - » Make sure you fully understand the trades you are doing
 - » Make sure a hedger does not become a speculator
 - » Be cautious about making the treasury department a profit center

References

- Ahoy, C. (199), “Process Mapping”, Facilities News, Iowa State University, September.
- B.I.S., Basel Committee on Banking Supervision (2003b), “Sound Practices for the Management and Supervision of Operational Risk”, Publication Nr.96, February.
- B.I.S., Basel Committee on Banking Supervision (2004), “International Convergence of Capital Measurement and Capital Standards – a Revised Framework”, BIS publications, June.
- Chapelle, A., G. Hübner and J.P. Peters, (2005), Le risque opérationnel : Implications de l’Accord de Bâle pour le secteur financier, Editions Larcier, coll. Cahiers Financiers, 2005, 155 p.
- Chapelle, A. Y. Crama, G. Hübner and J.-P. Peters (2008), “Practical Methods for Measuring and Managing Operational Risk in the Financial Sector: A Clinical Study” jointly with, Journal of Banking and Finance, forthcoming.
- James Lam & Associates, “Emerging best practices in developing Key Risk Indicators and ERM Reporting”, White Paper, 2006.