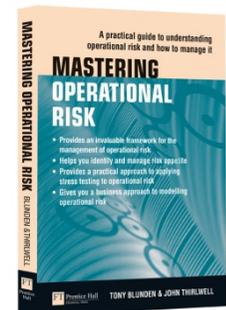


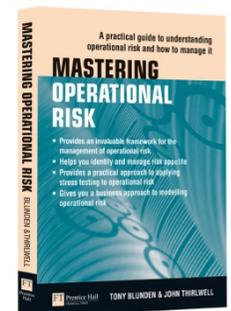
# Operational risk in Basel II and Solvency II

John Thirlwell

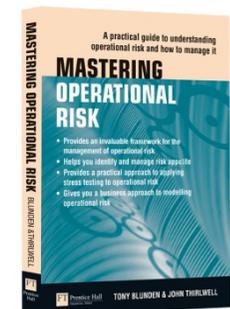
Royal Docks Business School, University of East London  
14 October 2010



- Operational risk and Basel II
  - Defining operational risk
  - Capital for operational risk
- Operational risk and Solvency II
- The operational risk management framework
  - Operational risk governance
  - Challenges for operational risk management
    - Operational risk appetite
    - Losses and events
    - Control self-assessments and scenarios
  - Qualitative modelling
- People risk



<b>Year</b>	<b>Event</b>
1812	Napoleon's retreat from Moscow
1912	Sinking of <i>Titanic</i>
1986	<i>Challenger</i> space shuttle
1986	Chernobyl nuclear reactor
1988	Piper Alpha oil rig (North Sea)
1988	Lockerbie terrorist air strike
1989	<i>Exxon Valdez</i> oil tanker
1993	Metallgesellschaft
1995	Barings Bank (Nick Leeson) (+ Daiwa, Sumitomo, Société Générale, Allied Irish, National Australia Bank)
1998	Long Term Capital Management
2000	Millennium Bug
2001	World Trade Center (9/11)
2001	Enron/Arthur Andersen
2003	SARS near-pandemic
2005	Hurricane Katrina
2010	Gulf of Mexico oil rig
2010	Eyjafjallajökull (Iceland) volcano



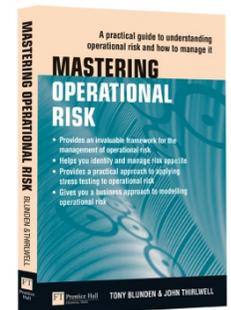
# Defining operational risk

‘Operational risk is the risk of direct or indirect losses resulting from inadequate or failed processes, people or systems, or from external events.’ [*Operational risk: the next frontier*. RMA/PriceWaterhouseCoopers, 1999]

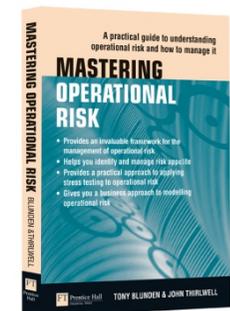
‘The risk of loss resulting from inadequate or failed internal processes, people or systems or from external events’ [Basel II]

- includes legal risk; excludes strategic and reputational risk
- regulatory risk?

‘The risk of loss arising from inadequate or failed internal processes, or from personnel and systems, or from external events.’ (Art 13 (33))



<b>BASEL II</b>	<b>SOLVENCY II</b>
Internal fraud	Intentional misconduct (internal fraud)
External fraud	Unauthorised activities by external parties (external fraud)
Employment practices and workplace safety	Employment practices and workplace safety
Clients, product and business practices	Clients, product and business practices
Damage to physical assets	External events that cause damage to physical assets
Business disruption and system failures	Business disruption and system failures
Execution, delivery and process management	Business process risks



# Basel II operational risk categories

## – Level 2 (1)

### Internal fraud

- unauthorised activity; theft (assets/IP), embezzlement, theft and fraud, insider trading (not on firm's account)

### External fraud

- theft and fraud; systems security breach/hacker

### Employment practices and workplace safety

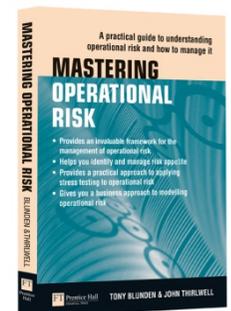
- employee relations; safe environment; discrimination

### Damage to physical assets

- including natural disasters

### Business disruption and system failure

- hardware, software, telecoms, utility outage



# Basel II operational risk categories

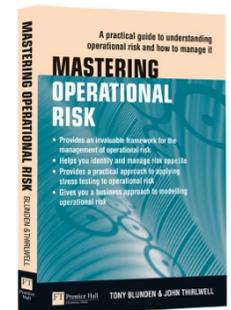
## Level 2 (2)

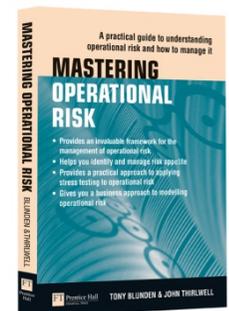
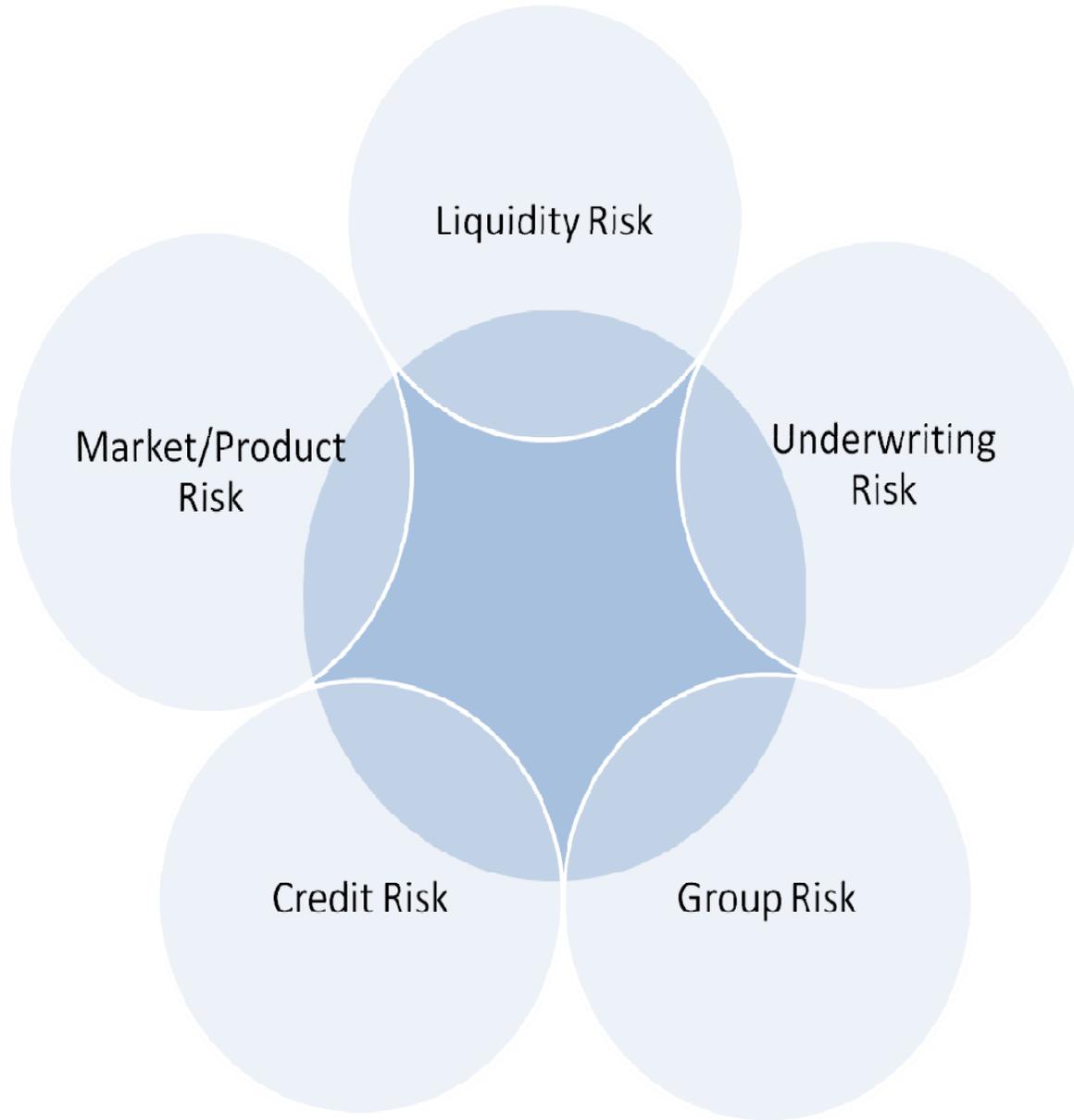
### Clients, products & business practices

- product suitability (incl KYC); fiduciary breaches; privacy breaches; lender liability; improper trade/market practices; money laundering insider trading (firm's account); product defects; model flaws; disputes over advisory activities; exceeding client exposure limits

### Execution, delivery & process management

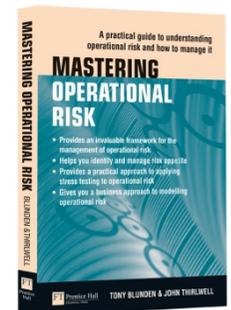
- transaction capture, execution and maintenance; data entry; delivery failure; collateral management failure; monitoring and reporting (incl external); documentation failures; customer/client account management; trade counterparties' disputes, non-performance; vendors and suppliers outsourcing and disputes



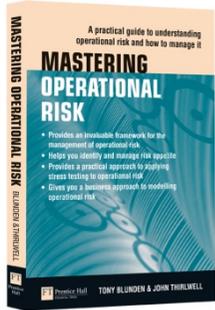
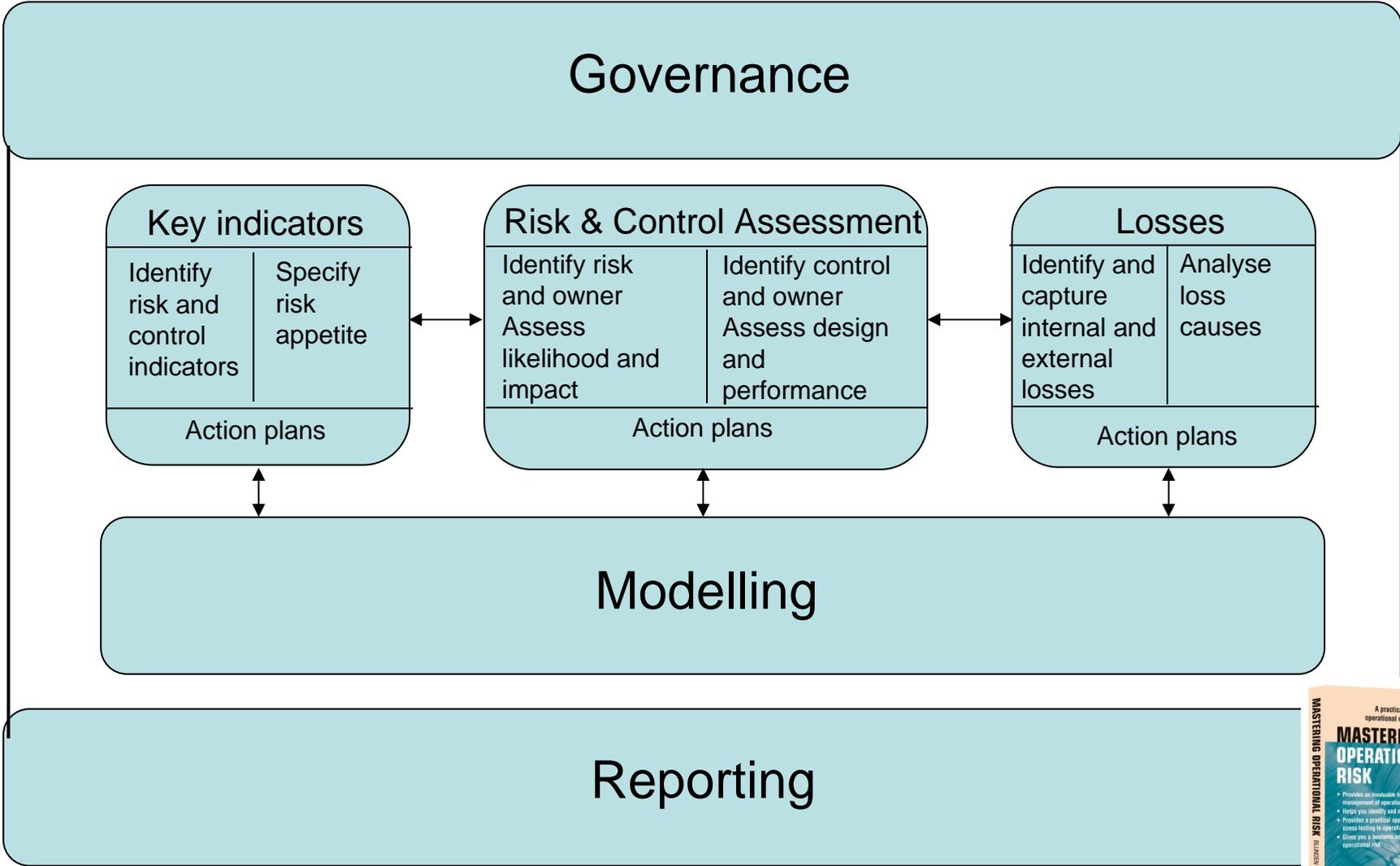


# Operational risk in Solvency II

- Definition of operational risk
- Capital rules for Solvency II
- The Own Risk Self Assessment (ORSA)
- The Internal Model
- The role of risk

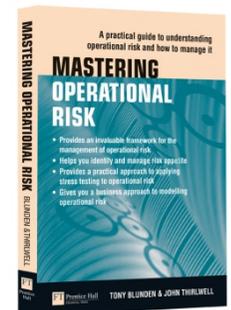


# ORM Framework

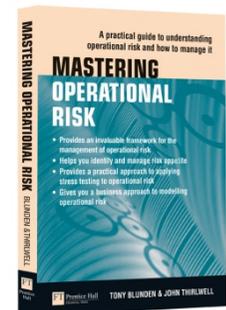
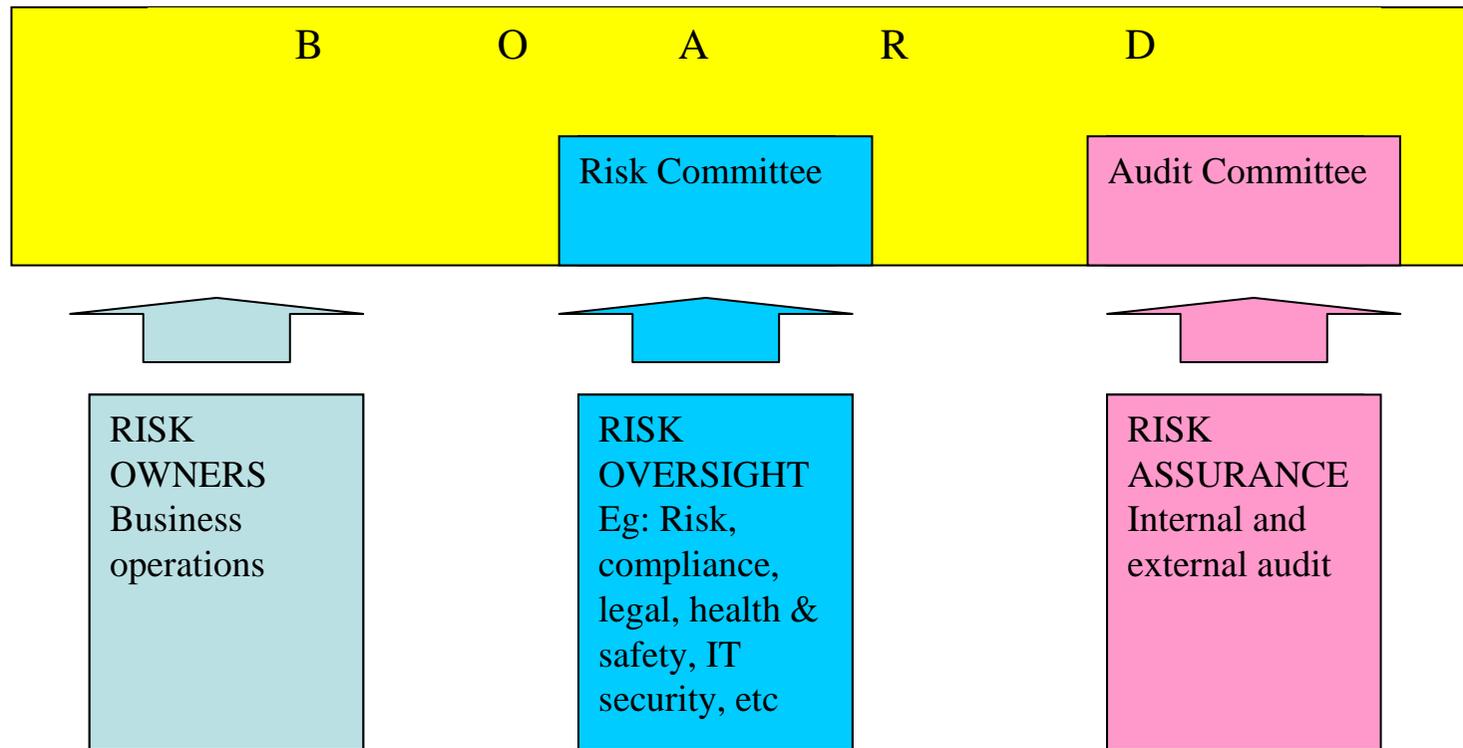


# Governance

- Getting the board on board
  - Leadership
  - Tone at the top; tune in the middle
  - Where does Risk sit?
    - Walker Report (Nov 2009)
      - Risk Committee
      - Chief Risk Officer
    - Where does Operational Risk sit?
- Reporting: colours and numbers

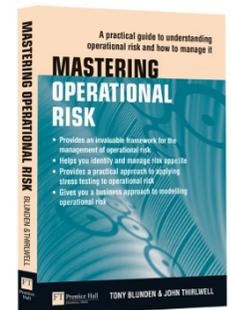


# Where does the operational risk function sit?

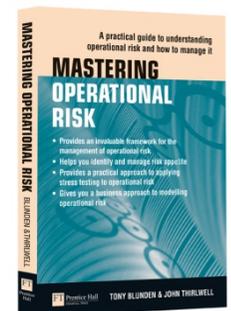
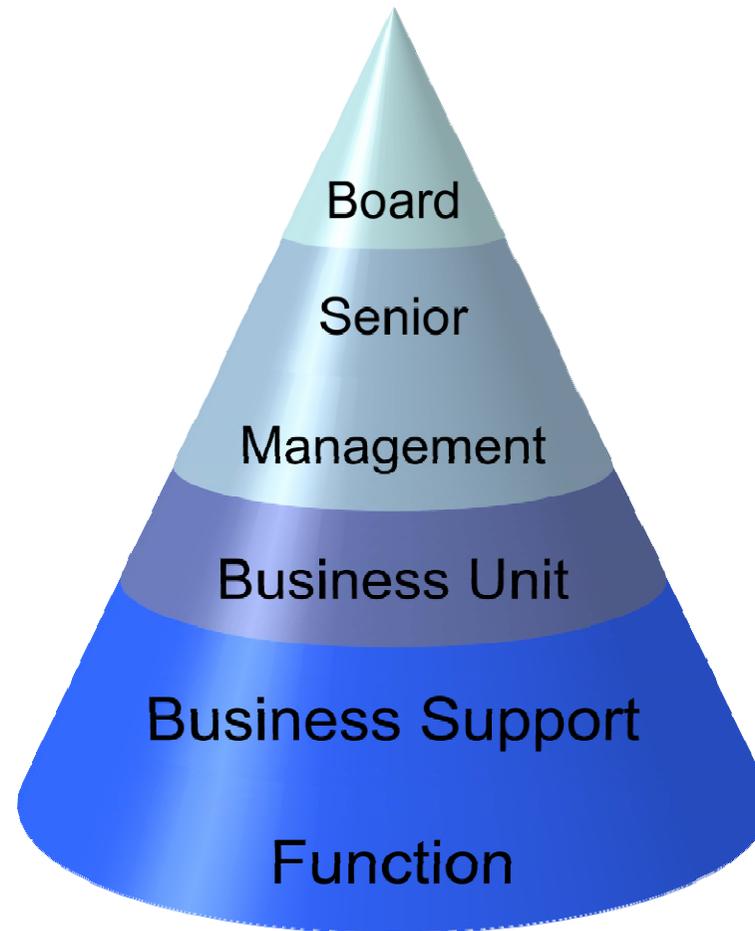


# Operational risk appetite (1)

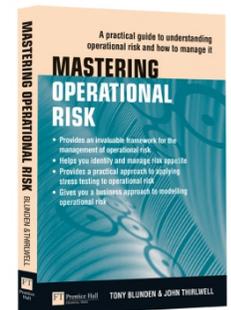
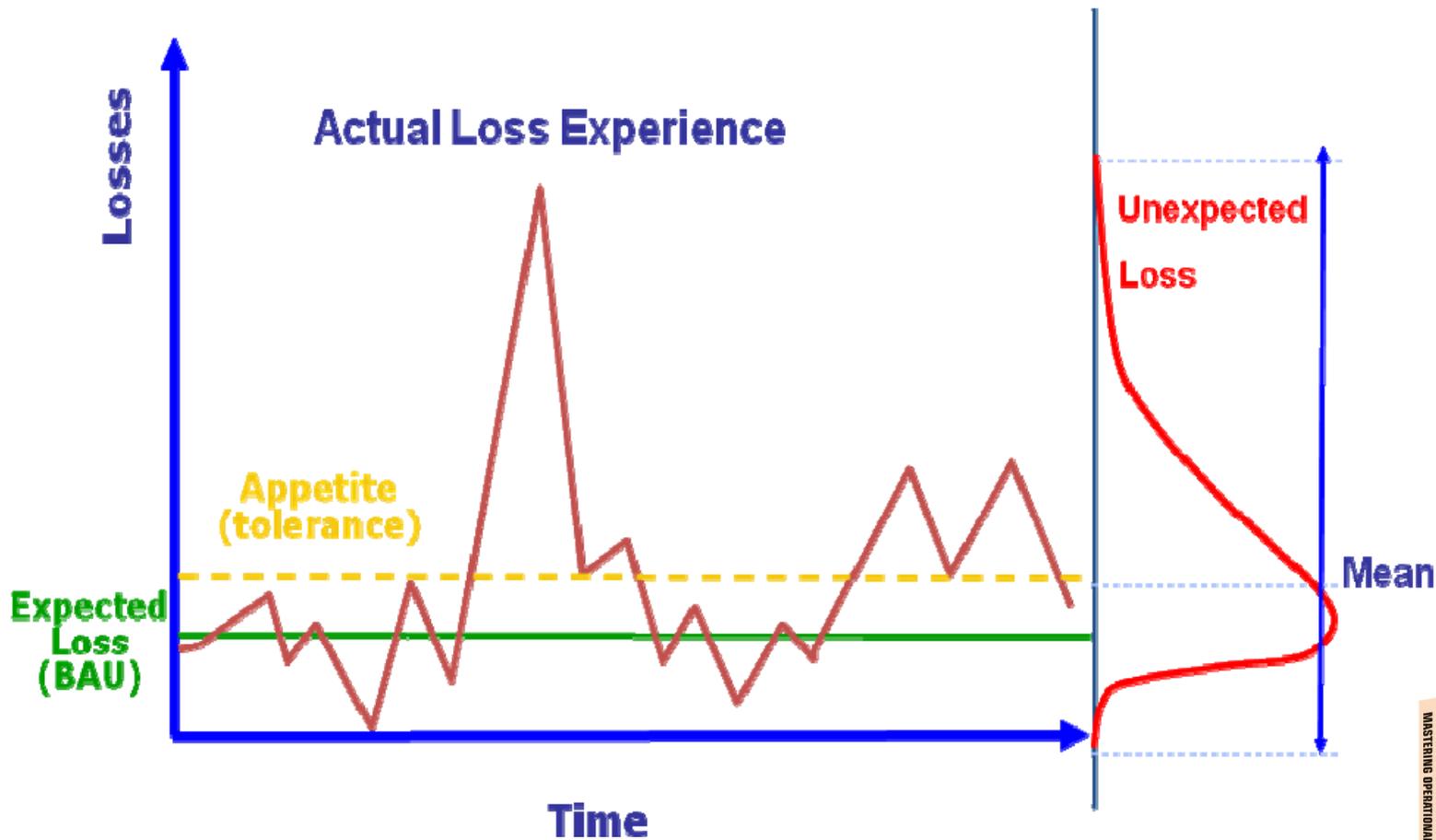
- Risk of loss a firm is willing to accept for a given risk-reward ratio [over a specified time horizon at a given level of confidence]
- No/minimal appetite for losses arising from financial crime, reputation, legal, regulatory events
- Unmitigated losses no more than  $x\%$  of PBT in any 3-year period
- No individual OR losses above  $\pounds x$  or cumulative losses above  $y$  over 12 month period. Losses above  $\pounds z$  to be reported to Risk or Audit Committees.



# Whose appetite is it anyway?



# Risk appetite in relation to loss experience (Fig 3.7)

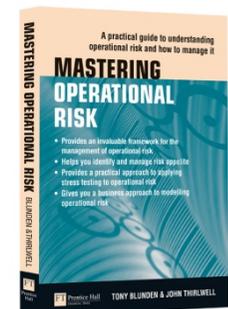


# Risk appetite using risk assessment scores (1) (Fig 3.8)

Annual Loss Thresholds	
Low	25,000
Acceptable	100,000
Warning	450,000
Catastrophic	1,500,000

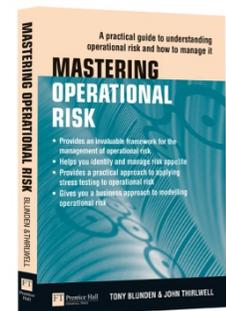
Impact per event (£)				
	<u>L'bound</u>	<u>U'bound</u>	<u>Mid point</u>	
Low	0	50,000	25,000	
Med-low	50,000	150,000	100,000	
Med-high	150,000	500,000	325,000	
High	500,000	1,500,000	1,000,000	

Likelihood of event (per annum)					
	<u>L'bound</u>	<u>U'bound</u>	<u>Alternative label</u>	<u>Mid point</u>	
Low	0.04	0.10	10% likely in next year	0.07	
Med-low	0.10	0.33	30% likely in next year	0.22	
Med-high	0.33	1.00	Very likely in next year	0.67	
High	1.00	12.00	Several times in next year	6.50	



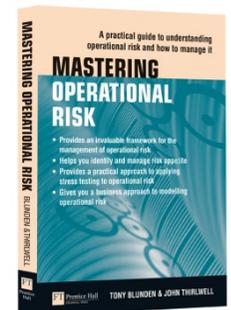
# Risk appetite using risk assessment scores (2) (Fig 3.9)

<b>IMPACT</b>	High	70,000	220,000	670,000	6,500,000
	Med-high	22,750	71,500	217,750	2,112,500
	Med-low	7,000	22,000	67,000	650,000
	Low	1,750	5,500	16,750	162,500
		10% likely	30% likely	Very likely	Severe
		<b>LIKELIHOOD</b>			

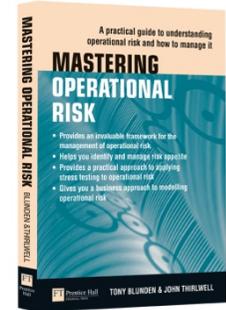


# Capital for operational risk

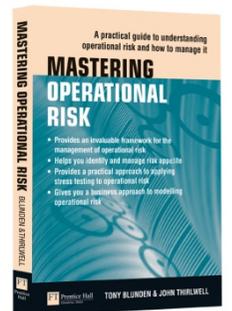
- Basel II (June 2004: 1/1/08)
  - Basic indicator approach (15% x Gross income)
  - Standardised approach (12-18% x Gross income)
  - Advanced Measurement Approach: 99.9% x 12 mths
- Basel III (Sept 2010: 2018)
- Solvency II
  - Standardised (% premiums + % expenses; cap of 30%)
  - Internal model: 99.5% x 12 months



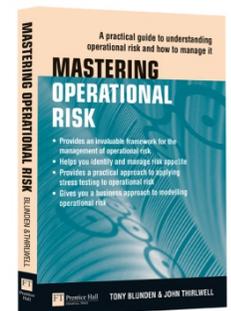
# Is operational risk different from other risks?



	Credit /market/ commodity/ liquidity risks	Operational risk
Is the risk transaction-based?		
Is the risk assumed proactively ?		
Can it be identified from accounting information e.g. the P&L?		
Can occurrence of the risk (all risk events) be audited?		
Can its financial impact be capped or limited?		
Can you trade the risk?		

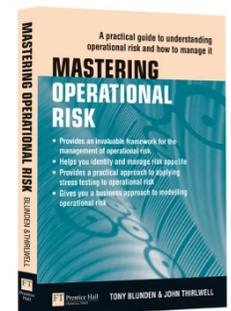


# Quantifying operational risk - loss event data



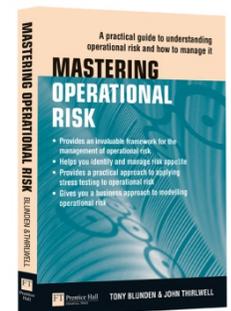
# Issues and decisions concerning loss data

- **Which losses?**
  - Reporting threshold
  - Near misses
  - “Boundary” losses



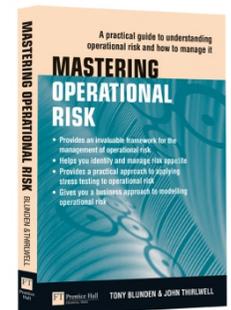
# Attributes of loss event data

- **Amount** – the basis of severity
  - Currency
  - Multiple events
  - Indirect costs: costs to fix? business interruption costs? foregone income?
  - Offsets and gains, i.e. gross/net?
- **Date** – the basis of frequency
  - Event / reporting date
  - Multiple events
- **Loss category**
- Business activity, business unit
- Geographical location
- **Effect/impact** – by type
- **Cause** – narrative/type



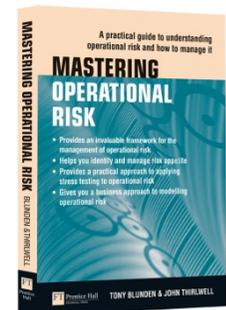
# Realities of loss event data

- It will be incomplete, scarce and patchy
- It will be inconsistently reported although, once reported, it *is* auditable.
- It is historic and backward looking. Major events will probably have led to tighter controls, change of policy etc.
- It does not, of itself, tell you about **causes**.



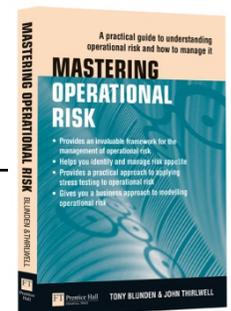
# Frequency and severity – Traditional ORM

High (3) <b>Frequency</b>	3	6	9
Med (2)	2	4	6
Low (1)	1	2	3
	Low (1) <b>Severity</b>	Med (2)	High (3)

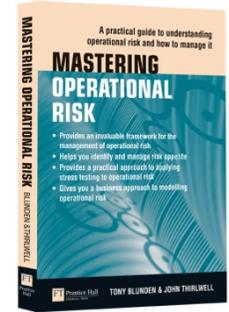


# Frequency and severity - modern ORM

High (3) Frequency		n/a	n/a
Med (2)			n/a
Low (1)			
	Low (1) Severity	Med (2)	High (3)



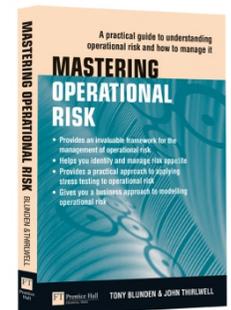
# Practical challenges



	Losses	Control risk self assessment
Objective (past)	Y	N?
Subjective (forward looking)	N	Y
Quality analysis by:	Finance	Management
Quantity available	Low?	Tailored
Collection time	Long	Short
Source	Accounts, but . . .	Management

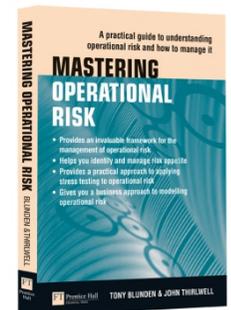
# Modelling operational risk - a qualitative approach

- Use existing risk and control assessments
- No need to wait for adequate loss history
- How it might work:
  - Set up ranges (see Risk Appetite slides)
  - Assess impact and likelihood of risks
  - Assess failure probabilities of controls
  - Correlate risks (if possible)
  - Challenge input
  - Run Monte Carlo simulations
  - Assimilate results and reports



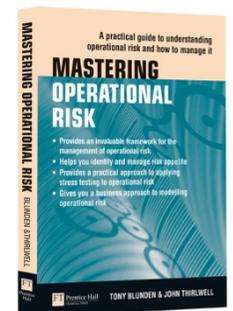
# People risk – the financial crisis

- Financial crisis
  - Failure to apply good risk management (credit, liquidity)
  - Failure to apply good risk governance
  - Asset bubble
  - Politicians, regulators, central banks
  - Human behaviour (greed, herd instinct)



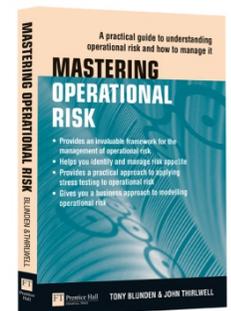
# The people risk environment

- Corporate strategy and objectives
- Excellent behaviour = ?
- Leadership and culture
- Openness and transparency
- Communication
- Change and flexibility



# Mitigating people risk

- Selection
- Appraisals and performance management
- Training and development
- Reward
- Succession planning
- OR and HR
- Key people risk indicators



# Contact details

**John Thirlwell**

**Tel: +44 (0) 208 386 8019**

**Mob: +44 (0) 781 382 9362**

**e-mail: [info@johnthirlwell.co.uk](mailto:info@johnthirlwell.co.uk)**

**[www.masteringoperationalrisk.com](http://www.masteringoperationalrisk.com)**

