

# Building a risk management framework

John Thirlwell

Sliema, Malta, 7 March 2009

- Identifying risks
- Losses and risk measurement
- Risk and control assessment
- Risk indicators
- Scenarios and stress tests
- Risk appetite and tolerance
- Reporting

# Identifying risks

## – where to start

- By risk type: operational, credit, market, liquidity etc
- Operational/business risk:
  - People (employee misdeeds, breaches of employment or health & safety legislation, workforce disruption);
  - Process (payment, settlement, compliance, assembly line);
  - [IT] Systems (development, capacity, failure, security);
  - External (disasters, infrastructure failure, criminal activity, outsourcing)
- Strategic; process (function/business unit); activity

## **Basel Loss Event Type Classification** (Levels 1 and 2)

Internal Fraud	Unauthorised activity Theft and fraud
External fraud	Theft and fraud Systems security
Employment practices and workplace safety	Employee relations Safe environment Diversity and discrimination
Clients, products and business practices	Suitability, disclosure and fiduciary Improper business or market practices Product flaws Selection, sponsorship and exposure Advisory activities
Damage to physical assets	Disasters and other events
Business disruption and systems failures	Systems
Execution, delivery and process management	Transaction capture, execution and maintenance Monitoring and reporting Customer intake and documentation Customer/client account management Trade counterparties Vendors and suppliers

- Identifying risks
- Losses and risk measurement
- Risk and control assessment
- Risk indicators
- Scenarios and stress tests
- Risk appetite and tolerance
- Reporting

# Attributes of loss event data

- Loss category
- Amount – the basis of severity
- Date – the basis of frequency
- Business activity, business unit
- Geographical location
- Cause - narrative
- Effect/impact

# Issues and decisions concerning loss data

- Reporting threshold
- Near misses
- Indirect costs
  - costs to fix
  - business interruption
  - foregone income
- Gains and offsets
- “Boundary” losses

# Internal loss event data – some health warnings

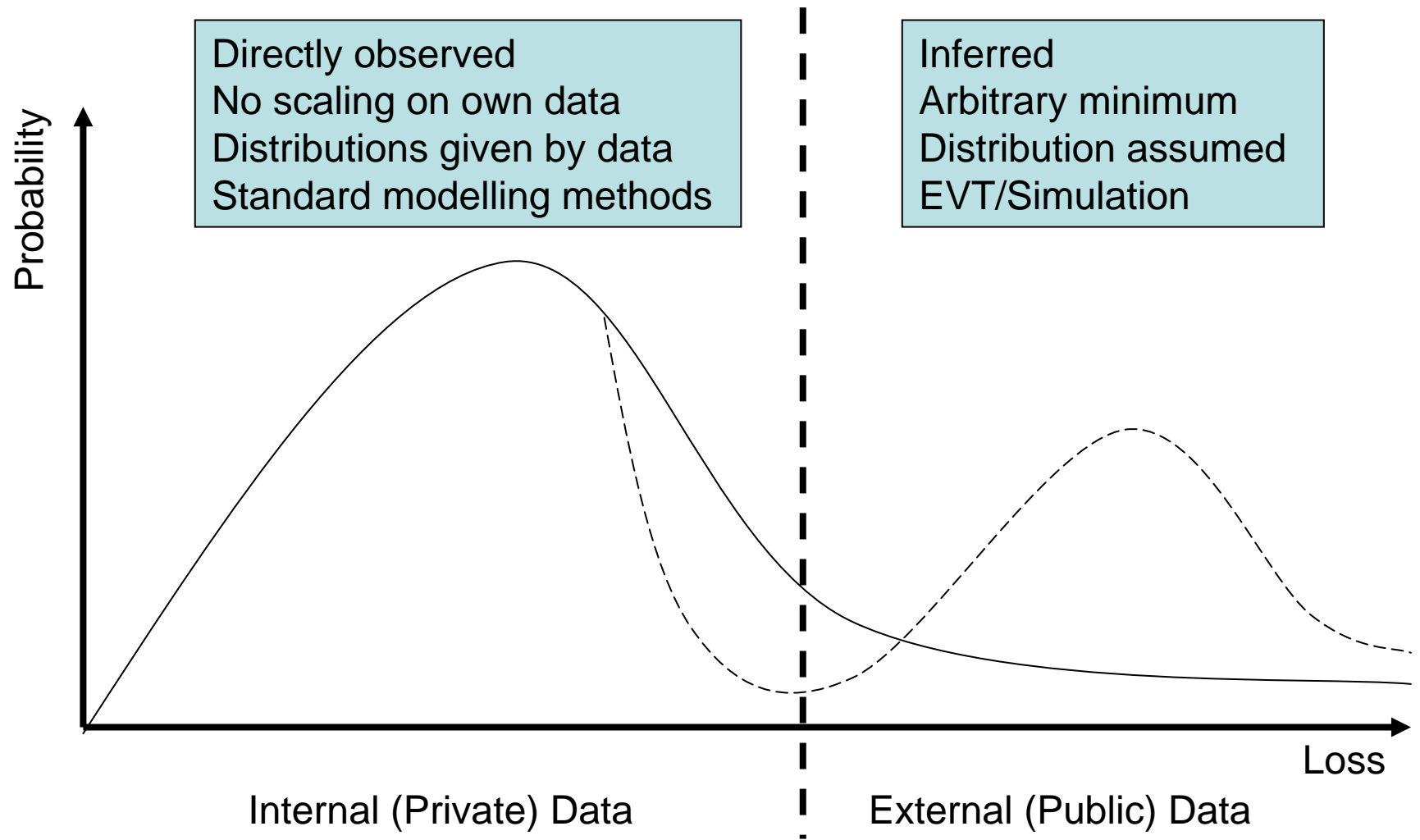
- It will be **incomplete**, be scarce and patchy
- It will be **inconsistently** reported although, once reported, it *is* auditable.
- It is **historic** and backward looking. Major events will probably have led to tighter controls, change of policy etc.
- It does not, of itself, tell you about **causes**.

But it can . . .

- Focus management attention on areas of activity that are giving rise to losses
- Validate risk self-assessments, key risk indicators, scenario analysis and capital allocation.
- It is therefore extremely useful as *information*.



# The Tail Problem



# External loss data

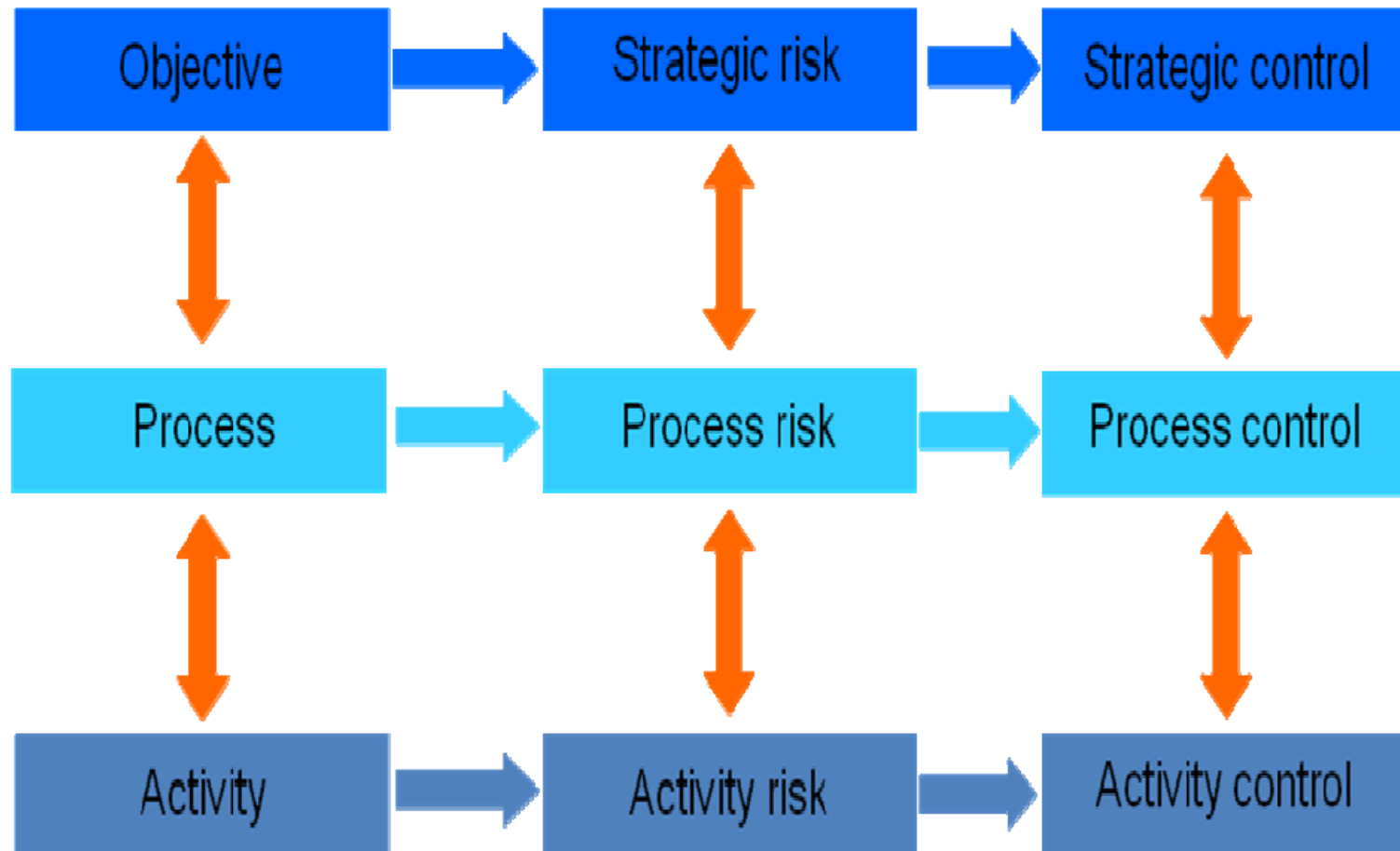
- Pooled (industry pools) and public (e.g. press) data
  - All the concerns of internal data
  - As with internal data, its construction and nature will depend on the purpose for which it is gathered (e.g. benchmarking; raw data; causal; modelling; informing scenario analysis)
  - Different risk, control and reporting cultures
  - Exclusions (e.g. legal, insurance settlements)
  - Scaling
- The use of external data
  - provide *information*
  - enhance risk management rather than measure “severe” losses
  - “External data is in the realm of *scenario analysis*” - Roger Cole, Chairman Basel Risk Management Group.

- Identifying risks
- Losses and risk measurement
- Risk and control assessment
- Risk indicators
- Scenarios and stress tests
- Risk appetite and tolerance
- Reporting

# Risk and control assessment

- A matrix to assess frequency/probability/likelihood and severity/impact.
- Involves some degree of scoring
  - Qualitative, e.g. traffic lights (red, amber, green) or H,MH,ML,L
  - Quantitative, i.e. € or € range for impact, or % or 1 in x years for frequency
  - how many grades?
- How often?

# Levels of risk and control assessment



# Frequency and severity – traditional view of risk

<i>Frequency</i> High (3)	3	6	9
Medium (2)	2	4	6
Low (1)	1	2	3
	Low (1) <i>Severity</i>	Medium (2)	High (3)

# Frequency and severity - modern risk management

<i>Frequency</i> High (3)		n/a	n/a
Medium (2)			n/a
Low (1)			
	Low (1) <i>Severity</i>	Medium (2)	High (3)

# Matrix parameters – an example

<b>Frequency</b>	
<i>Definition</i>	<i>Expected frequency</i>
Almost impossible	< 1 x 10 years
Rare	Between 1 x 1 yr and 1 x 10 years
Very unlikely	Between 1 x 1 month and 1 x 1
Unlikely	year Between 1- 5 x 1 month
Likely	Between 5 – 9 x 1 month
Very likely	> 9 x 1 month
<b>Severity</b>	
<i>Definition</i>	<i>Loss range</i>
Very severe	> 1000k
Severe	100k – 1000k
Moderate	10k – 100k
Small	1k – 10k



# What should impact relate to?

- Profit and loss?
  - sales
  - net income
- Shareholder value?
  - assets
  - capital
- Over what period?

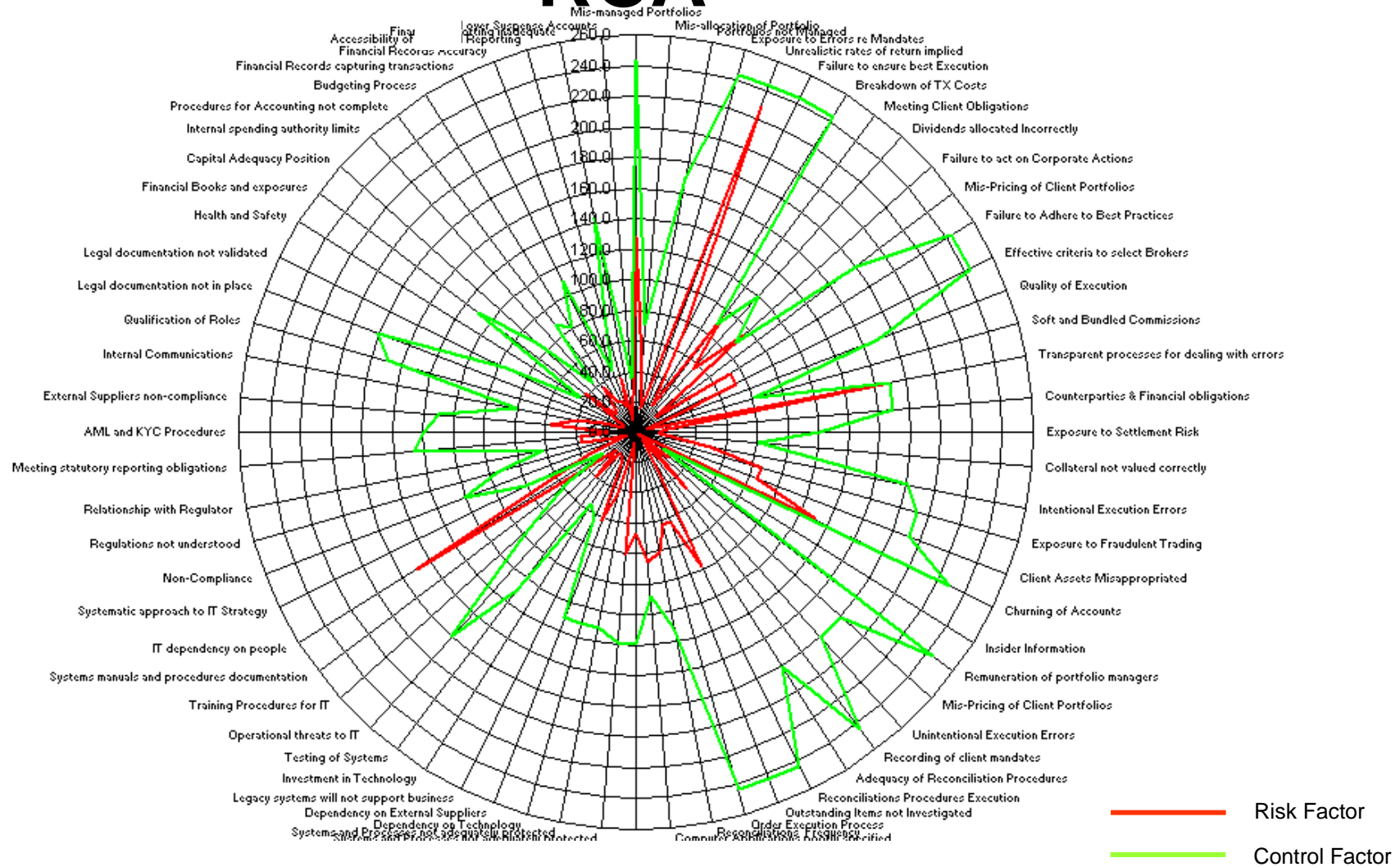
# Controls

- Preventative – tend to reduce likelihood of a risk occurring
- Detective or corrective controls – tend to reduce the impact a firm suffers

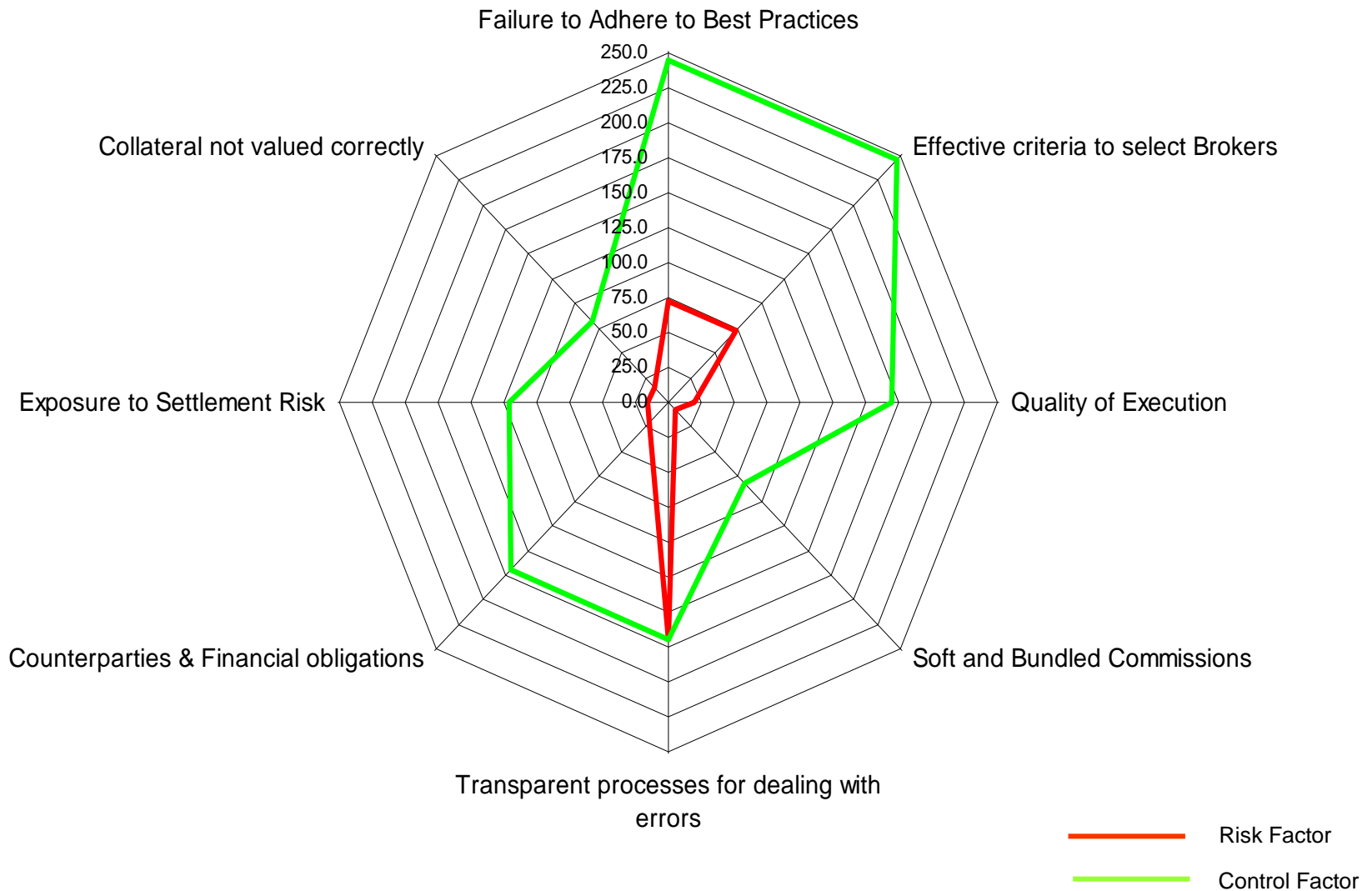
# Control (and risk) assessment

- Two assessments are required
  - assuming controls fail (gross/inherent)
  - assuming controls work (net/residual)
    - includes assessment of the controls for design and performance (i.e. effectiveness in reality)
- To assess controls:
  - Identify at suitable level (strategic, process, activity)
  - Look for independent rather than linked controls
- The final result will provide
  - A 'league table' or representation of risk exposures, which will drive management *action* and provide the basis for *evaluations* of new controls
  - A risk map for senior management
  - Feeds to internal and external auditors regarding the effectiveness or weaknesses in controls

# RCA



# Organisational Risk & Control Factors



# Practical challenges

	<b>Losses</b>	<b>RCSA</b>
Objective (past)		
Subjective (forward looking)		
Quality analysis by:		
Quantity available		
Collection time		
Source		

# Practical challenges

	<b>Losses</b>	<b>RCSA</b>
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

- Identifying risks
- Losses and risk measurement
- Risk and control assessment
- Risk indicators
- Scenarios and stress tests
- Risk appetite and tolerance
- Reporting



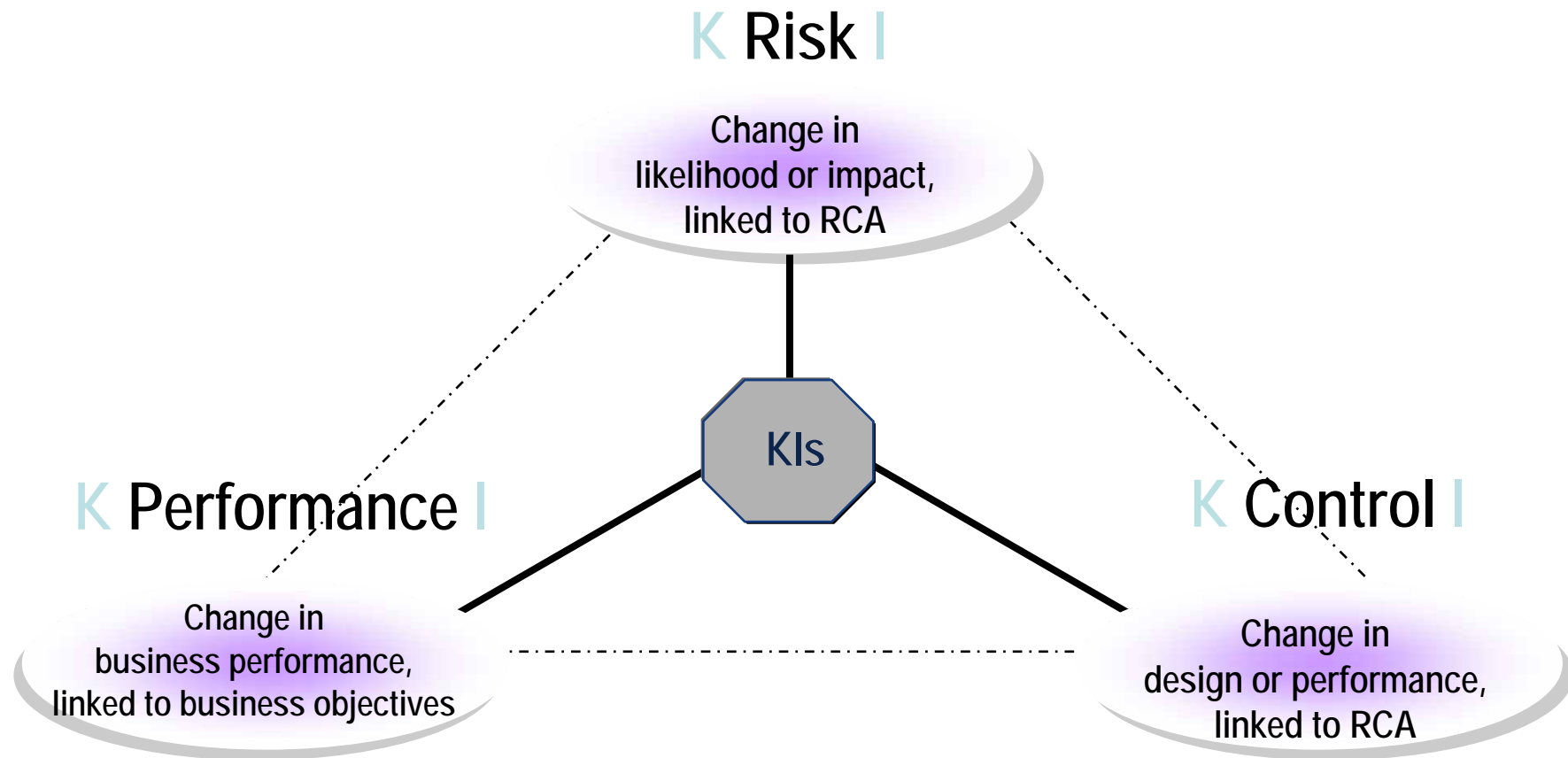
# What is (and is not) a KRI

---

- Observed or calculated values used to show the state of a risk which is considered key.
- A warning light of future risk exposure.
- Measures trends.
- Identifies factors which have not yet become events.
- Enables early detection and management of unacceptable risk in each function or process against predefined tolerance levels.
- Should be a meaningful driver of risk (ie related to *causal* factors)
- NOT:
  - A predictor of future risk severity or frequency
  - An indicator of control or control failure
  - An indicator of business performance

# Indicators

---



# KRI examples (1)

- People: turnover, temporary staff %, overtime, client complaints, absenteeism, staff satisfaction, training realisation, holiday patterns, vacancies
- Processing: failed & overdue settlements, claims & complaints, manual bookings
- Accounting: suspense accounts, corrections, manual bookings, large unusual transfers, budget overruns

# KRI examples (2)

- Controls: mandate deviations, error tracking, number & size of limit excesses
- Systems: downtime, project management, change releases
- Documents: corrections, text-omissions, backlogs, complaints
- Compliance: money laundering cases, investigations, audit issues outstanding

# Working with the business

- Talk to the business about its risks and its current indicators
- Find out what indicators are significant
- Separate risk, control and performance indicators
- 60% to 70% of indicators for key risks are in the businesses already

# EXERCISE

# Risk indicators - an Audit Committee perspective

## NB almost all Y/N

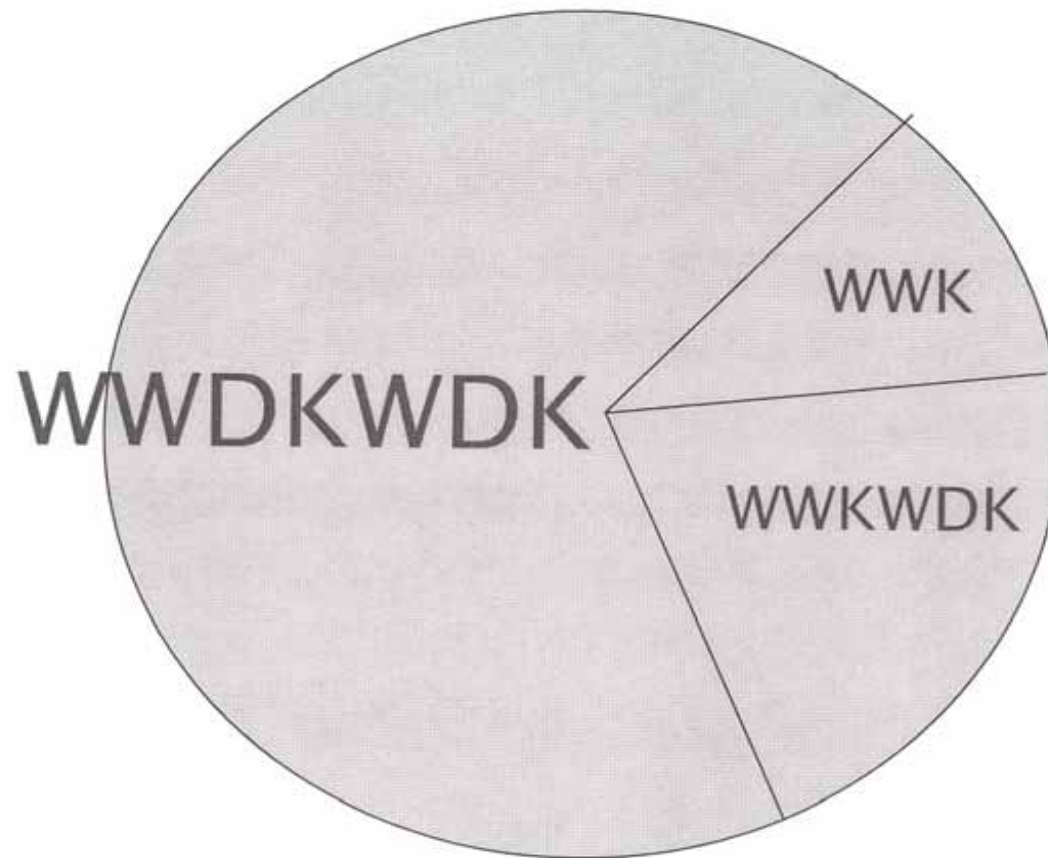
[Audit Committee Institute (KPMG) – Shaping the Audit Committee agenda, May 2004]

Inappropriate tone at the top	Unusually rapid growth
Frequent organisational changes	Unusual results or trends
High turnover of senior mgt	Industry softness or downturns
Lack of succession plans	Interest rate or currency exposures
Inexperienced management	Exposure to rapid technological changes
Lack of management oversight	Late surprises
Management over-ride	Autocratic management
Overly complex organisational structures or transactions	Ongoing or prior investigations by regulators or others
Untimely reporting and responses to audit committee enquiries	Excessive or inappropriate performance-based compensation
Unrealistic earnings expectations (by firm or financial community)	Lack of transparency in business model and purposes of transactions

- Identifying risks
- Losses and risk measurement
- Risk and control assessment
- Risk indicators
- Scenarios and stress tests
- Risk appetite and tolerance
- Reporting



# An Uncertain World



not forgetting **WWDKWK**

# Scenario analysis

- Scenarios are about assessing tail events i.e. the 1 in 100/200 (99/99.5% confidence) year event
- Tail events generally result from:
  - Several controllable things going wrongOr:
  - An uncontrollable external catastrophe(s).Very occasionally
  - A combination of the above.
- Scenarios should represent combined events and attempt to cover different types of risks to the firm.
- They are stories, so are readily understandable,  
e.g. . . . . .

# Combined scenarios

## – examples from insurance

- Wording dispute – major claim conceded. Other policies with same wording expose insurer to further unexpected claims. Staff levels at firm not sufficient to process claims volumes. Work-force overworked. Senior claims manager leaves; replacement cannot be found for 12 months.
- Loss of largest underwriting team to competitor. Profitable niche market, so high recruitment costs and long lead time resulting in loss of profits. Poor maintenance of documentation resulting in inability of firm to fully service claims.
- Bomb in City. Major damage to insurer and to Lloyd's building. Access to Lloyd's building denied for extended period. Loss of life of key underwriters and/or senior management. BCP invoked. Firm not running at full capacity.

# Stress tests

- For specific risks we use stress tests
- What is the appropriate timescale – 10 years, 20 years, 200 years?
- 1 in 10 years could lead to:
  - Equities: 30%
  - Interest rates:  $\pm$  200 basis points
  - Credit default: expected + 1 std. deviation
  - New business: +50%
  - Combinations: equities – 15%, interest rates + 100 basis points
  - 30/40% drop in house prices (FSA, November 2006)

- Identifying risks
- Losses and risk measurement
- Risk and control assessment
- Risk indicators
- Scenarios and stress tests
- Risk appetite and tolerance
- Reporting

# Risk appetite definition

The amount that a firm is willing to risk  
(for a given risk-reward ratio)

# What does risk appetite mean in the context of risk?

- Can a limit be put on all risks?
- Is zero reasonable – or meaningful?
- Must an “appetite” be capable of measurement, ie be a metric?
- If or where the answer is NO to the above, what do we mean by risk appetite? How do we manage it?

# Expressing risk appetite in risk policies

- Direct financial loss, or specific measures
- Non-financial statements
  - The Group's appetite for operational risk is that which achieves a satisfactory trade-off between the level of risk and the size of the likely returns. This principle applies across all types of operational risk loss and decisions on operational risk appetite must always be taken on the basis of this cost/benefit analysis.
- Appetite and tolerance
  - Continuity plans exist for business critical areas. The plans aim to ensure that, following an event, the Group is open for business the next working day and addresses the timely resumption of business as usual. The Group has no appetite for periods beyond those specified in the plans.
  - There is no appetite for reputational risk. On all outward announcements the group chief executive has to approve the final wording *or*  
The Group has no appetite for adverse media coverage and will use every effort to ensure that events that could potentially lead to such coverage are avoided

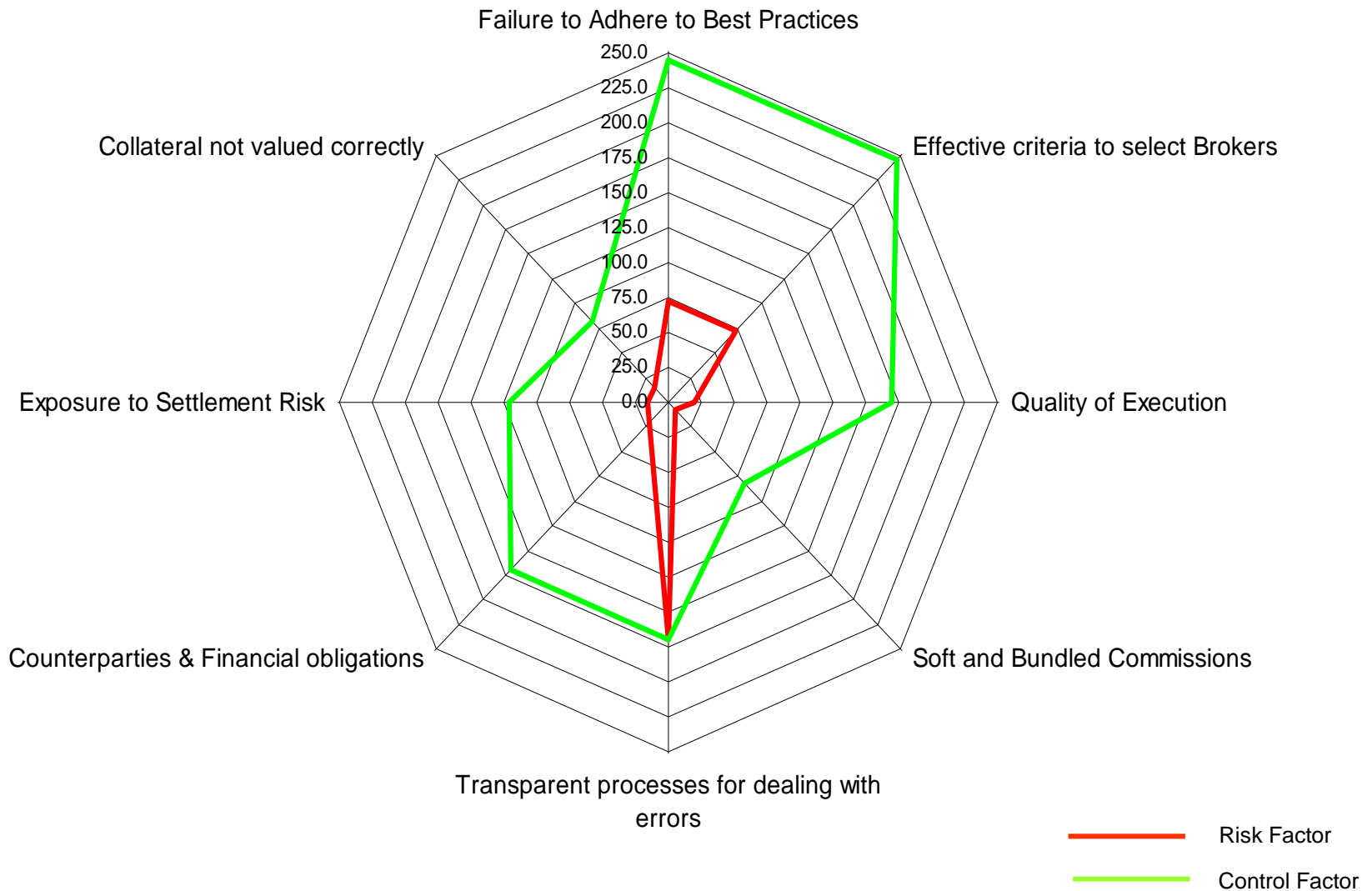


# Risk Appetite and business optimisation


Each of the four major processes can be used:

- Risk and control assessment
- Key indicators (both risk and control)
- Losses
- Scenarios

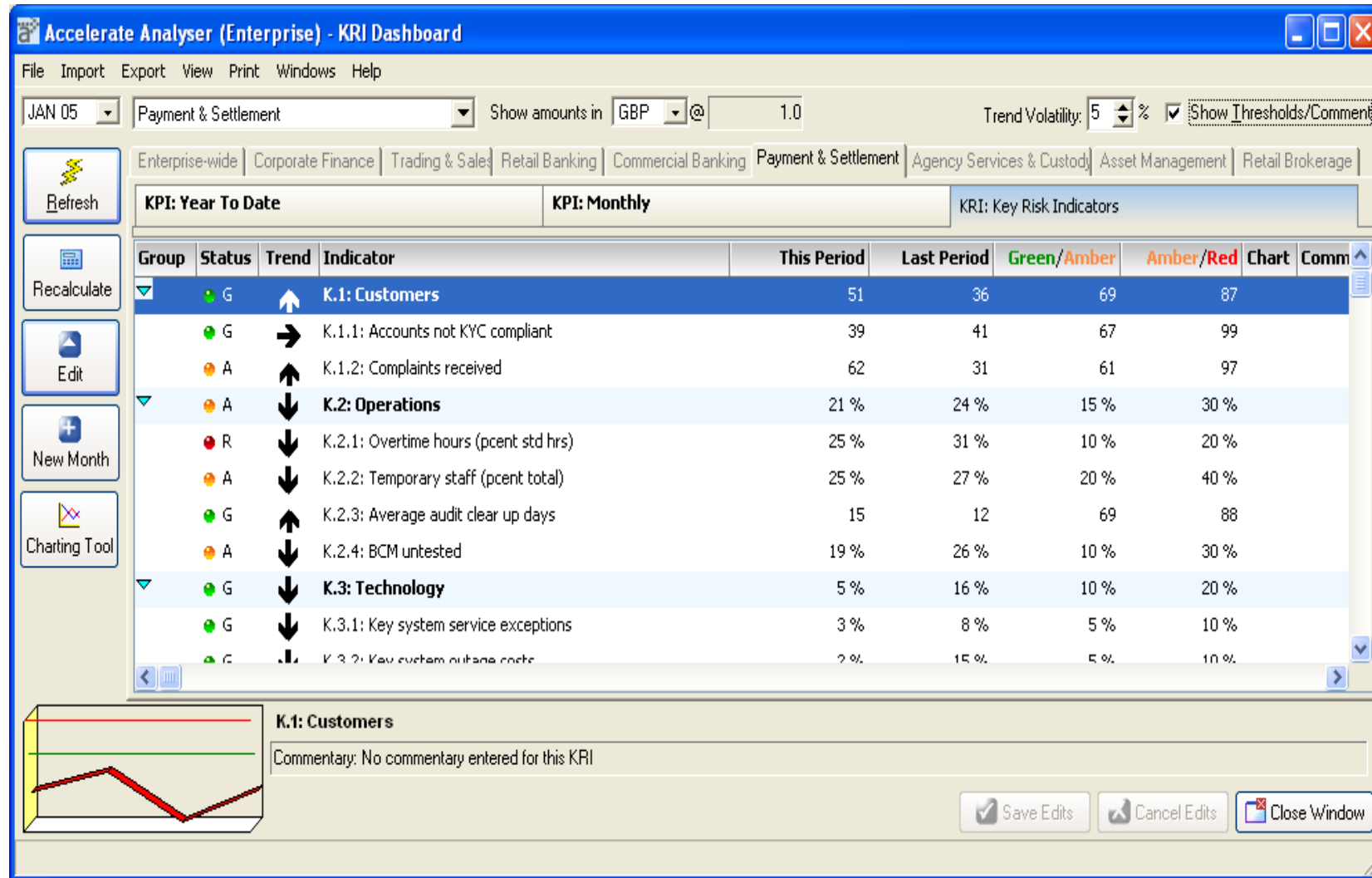
# Organisational Risk & Control Factors



# Value of Controls

	Mean Loss without Controls	Mean Loss after Controls	Control Efficiency %	Mean Value of Control
Risk 1	36,159	22,092	39	14,067
Risk 2	35,136	7,704	78	27,432
Risk 3	49,776	5,055	90	44,721
Risk 4	5,859	1,716	71	4,143
Risk 5	3,201	225	93	2,976
Risk 6	1,659	147	91	1,512
Risk 7	1,851	165	91	1,686
Risk 8	5,484	2,808	49	2,676
Risk 9	3,162	2,457	22	705
Risk 10	2,208	489	78	1,719
Risk 11	375	63	83	312
Risk 12	246	66	73	180
Risk 13	282	225	20	57
Risk 14	132	21	84	111
<b>TOTALS</b>	145,530	43,233		102,297

# Indicators



# Key (risk) indicators

<u>Key Indicator data</u>	<u>Period</u>	<u>YTD</u>	<u>Target for YTD</u>	<u>General Trend</u>	<u>Importance</u>
Staff Turnover rate against forecast (E)	2006	6	12	Stable	Low
Morale Tracker (Satisfaction Levels) (E) - 'staff surveys etc'	2006	Satisfied	Very Satisfied	Improving	Medium
Average Age (E)	2006	45 years	35 years	Improving	High
Staff Capability/Training (S)	2006		Highly Qualified	Worsening	High
<b>(E) Existing KI</b>					
<b>(S) Suggested KI</b>					
<u>Event experience</u>	<u>Date of Loss</u>	<u>£1000's</u>	<u>Provision / Budget</u>	<u>Unexpected Loss</u>	
Loss of 4 people from the Technology Department	2006	50	185	0	
<b>Totals</b>		<b>50</b>	<b>185</b>	<b>0</b>	

# Losses

Accelerate ECO (Economic Capital Optimiser)

Source Data | Goodness of Fit | What If | Correlations | **Outputs** | Chart

**View**  
 Confidence Interval: 99.9  
 View in: 000's  
 Calculate

**Selected Cell**  
 Corporate Finance  
 Internal fraud  
 Total Losses: 8,437,773  
 Expected Loss: 4,638,291  
 Capital Charge: 3,799,482  
 ↑ Current View

	Internal fraud	External fraud	Employment Practices & Workplace Safety	Clients, Products & Business Practices	Damage to Physical Assets	Business Disruption & System Failures	Execution, Delivery & Process Management	TOTAL
<b>Corporate Finance</b>	3,799	2,074	16,458	1,809	5,577	5,277	4,666	39,660
Trading & Sales	3,871	5,854	2,152	5,189	4,106	2,484	5,735	29,391
Retail Banking	7,745	8,667	7,039	1,424	3,124	11,723	7,517	47,239
Commercial Banking	5,445	5,571	3,263	804	3,184	1,041	2,847	22,155
Payment & Settlement	4,758	7,506	360	897	3,482	1,573	5,872	24,448
Agency Services	8,476	6,576	1,888	7,077	9,521	16	4,072	37,626
Asset Management	6,439	11,181	1,890	5,885	1,499	5,349	7,221	39,464
Retail Brokerage	1,165	6,150	9,787	5,915	5,634	12,289	1,667	42,607
<b>TOTAL</b>	41,698	53,579	42,837	29,000	36,127	39,752	39,597	282,590

Quit

# Risk and Control Assessment (annual loss)

## Annual Loss Thresholds

Low	25,000
Acceptable	100,000
Warning	450,000
Unacceptable	1,500,000

## Expected Loss Per Event

£	Lbound	Ubound	Alternative label	Mean
Low	250	1,000	Low	625
Medium/Low	1,000	5,000	Medium/Low	3,000
Medium	5,000	50,000	Medium	27,500
Medium/High	50,000	100,000	Medium/High	75,000
High	100,000	1,500,000	High	800,000

## Annual Frequency

frequency	Lbound	Ubound	Alternative label	Mean
Once / 5 yrs	-	0.20	Rare	0.10
Once / 2 yrs	0.20	0.50	Low	0.35
Once a yr	0.50	1.00	Moderate	0.75
Once a month	1.00	12.00	Very Likely	6.50
Once a day	12.00	365.00	Almost Certain	188.50

## Monetary (Mid)

	Once / 5 yrs	Once / 2 yrs	Once a yr	Once a month	Once a day
High	80,000	280,000	600,000	5,200,000	150,800,000
Medium/High	7,500	26,250	56,250	487,500	14,137,500
Medium	2,750	9,625	20,625	178,750	5,183,750
Medium/Low	300	1,050	2,250	19,500	565,500
Low	63	219	469	4,063	117,813

# Further thoughts on risk appetite

- There will be appetites for every risk
- They will be based on an assessment of risk and the cost (including quality) of 'controls'.
- Even where the appetite is zero (often involving risks which cannot be avoided), determine levels of *tolerance* which, again, will be subject to cost-benefit analysis.
- There will certainly not be a universal number or universal approach.

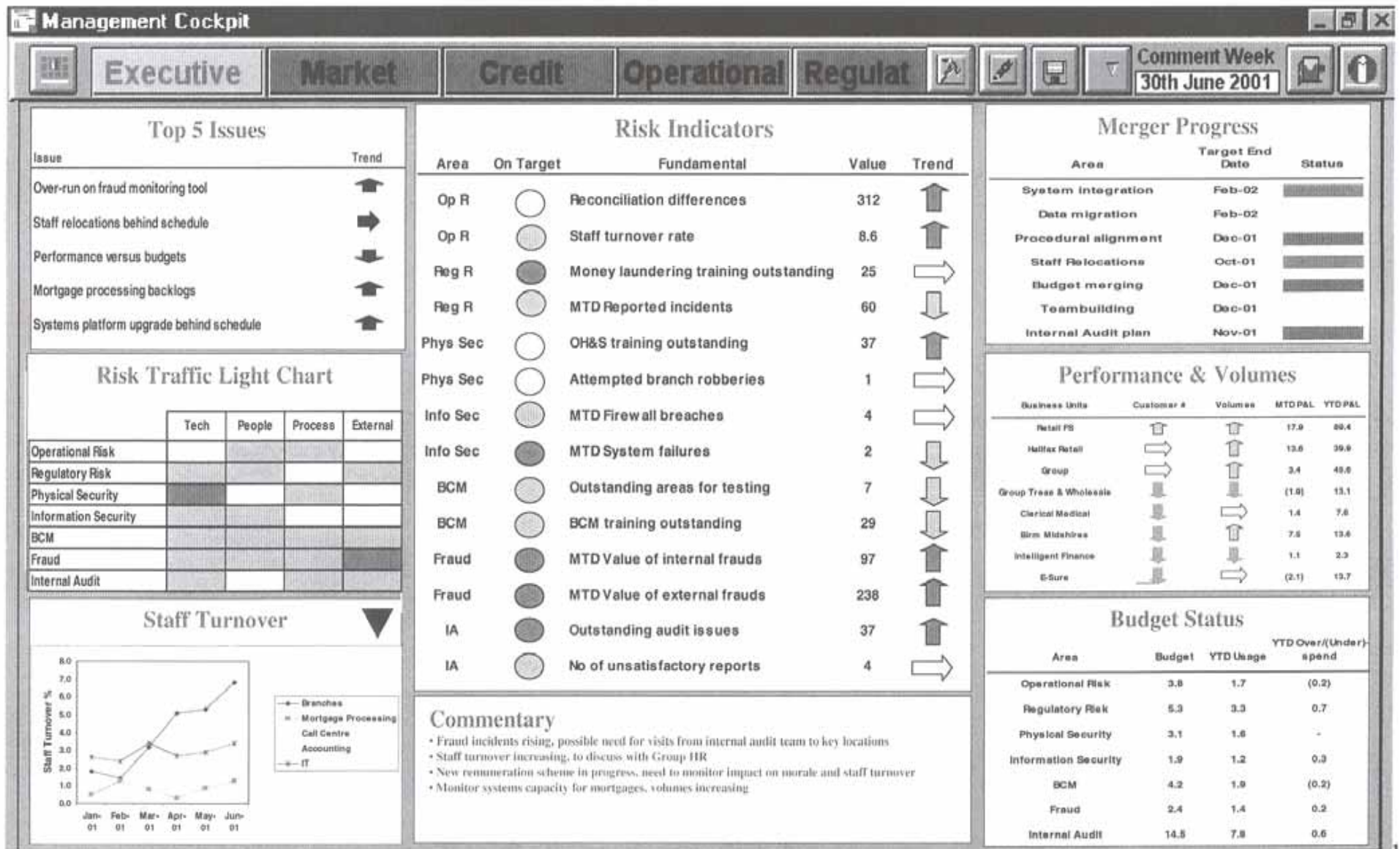


- Identifying risks
- Losses and risk measurement
- Risk and control assessment
- Risk indicators
- Scenarios and stress tests
- Risk appetite and tolerance
- Reporting

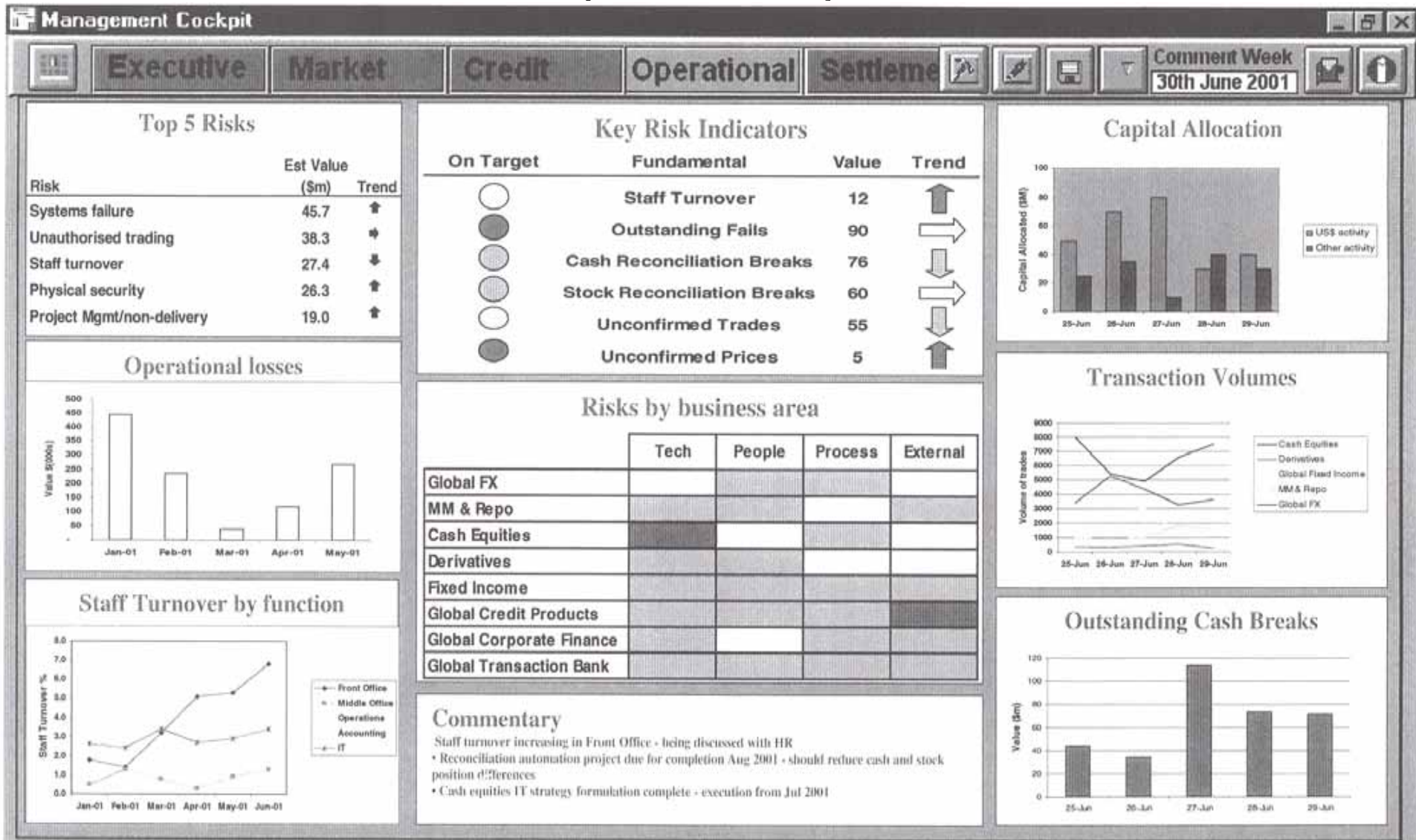
# Minimum requirements for risk reporting

High level risk description	Clear risk description of critical risks in rank order.
KPI/KRI pressure/direction	Are my warning signs of risk going up or down?
Risk severity assessment and movement – gross/inherent	How have we assessed the severity of the risk? Against what criteria?
Risk severity assessment and movement – net/residual	Do we understand the inherent risk?
Controls - appropriateness	Is the risk controllable? Do we have the right controls in place?
Controls - effectiveness	Do they work?
Controls - score	
Agreed action - progress	What actions have we agreed? Are we on track to deliver?
Owner	Do we have a single risk owner at executive level?
Oversight	By whom and how often?
Reports	Do we need more detailed information about critical risks?

# Executive dashboard (level 1)

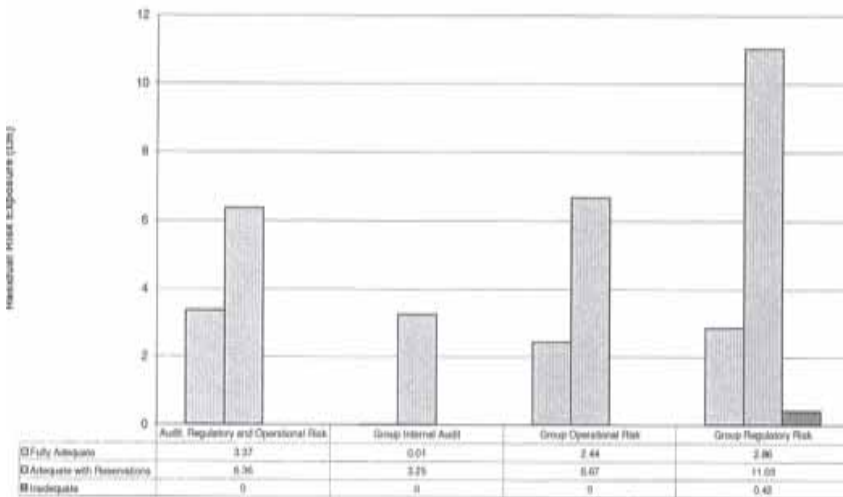


# Operational dashboard (level 2)

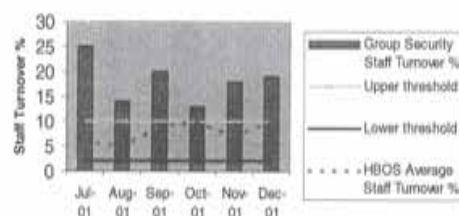


# Core systems report (level 3)

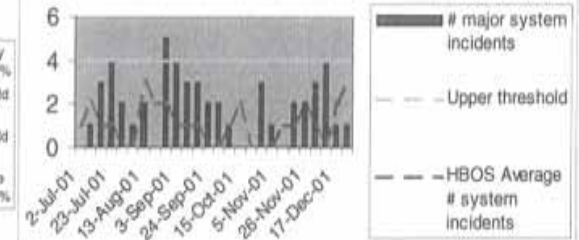
Residual Risk Exposure by Control Adequacy - Audit, Regulatory and Operational Risk as at 30th June 2003



Group Security - Staff Turnover %

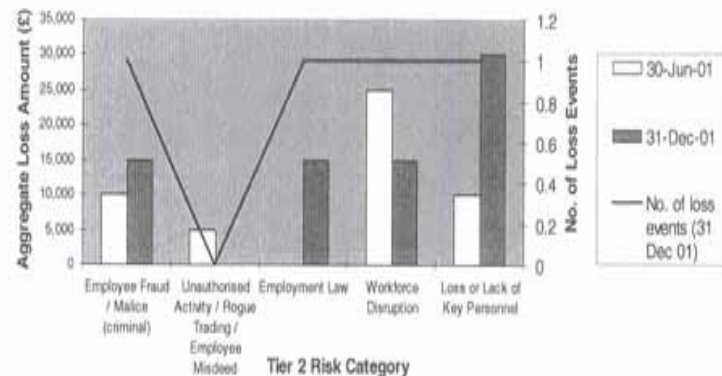


Group Security - Number of Major System Incidents



Mandatory Fields Indicated by (*)				
*Organisation Unit	Audit, Regulatory and Operational Risk			
<b>Risk Record</b>				
*Review Period	Status	*Risk Type	Risk No	Key Risk
31st Dec 2003	No Action Taken	Adopted	18036	Yes
*Risk Owner	Ammy Seth/Arthur Selman/David Fryatt			
*Risk Title	The risk that the technology does not deliver the intended benefit due to ineffective project management or non-performance from a service provider.			
Risk Description	The risk that ineffective project management leads to key functionality being absent from the system or significant time delays in implementation, together with increased costs. Alternatively, lack of control and influence over a non performing service provider (e.g. GBS, Algorithmics, SunGard) leads to the same result as above.			
<b>Risk Record - Details</b>				
* Risk Category - Tier 1	Risk Category - Tier 2	Risk Category - Tier 3		
Systems	Systems Development and Implementation	No Option Selected		
*Potential Causes	*Potential Impacts			
Insufficient service provider resource Insufficient service provider skill sets Poorly defined specifications Poor build of systems Poor delivery process Lack of co-ordinated approach by GAROR in using limited GBS resource	Non delivery of core functionality Users select alternative solutions - groupwide disparity Data reported are inaccurate/misleading Regulatory scrutiny Non Basel compliant			
*Current Controls	Control Weaknesses			
3rd party agreements and SLA's Steering committee for OpData Project Minimum Standards Group PPG GORRC RMDF DRWP	Ineffective SLA with service providers, leading to lack of control and influence over resourcing decisions made by internal or external service providers			

Loss Events by Tier 2 Risk Category



# John Thirlwell

Tel: +44 (0)20 8386 8019

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