

Enterprise-wide risk management in the insurance industry: Building a risk structure

John Thirlwell

Non-executive Director, Novae Syndicates Limited

Incisive Media, Köln, 23 November 2006

What is ERM?

- “A process, effected by an entity’s board of directors,. . . applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of its entity objectives.” [COSO]
- “A structured, consistent and continuous process across the whole organisation for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.” [Sumitomo Mitsui Banking Corp]
- “. . . the competence of a company to manage risk consistently across all disciplines.” [Donald Macdonald Partnership LLP]

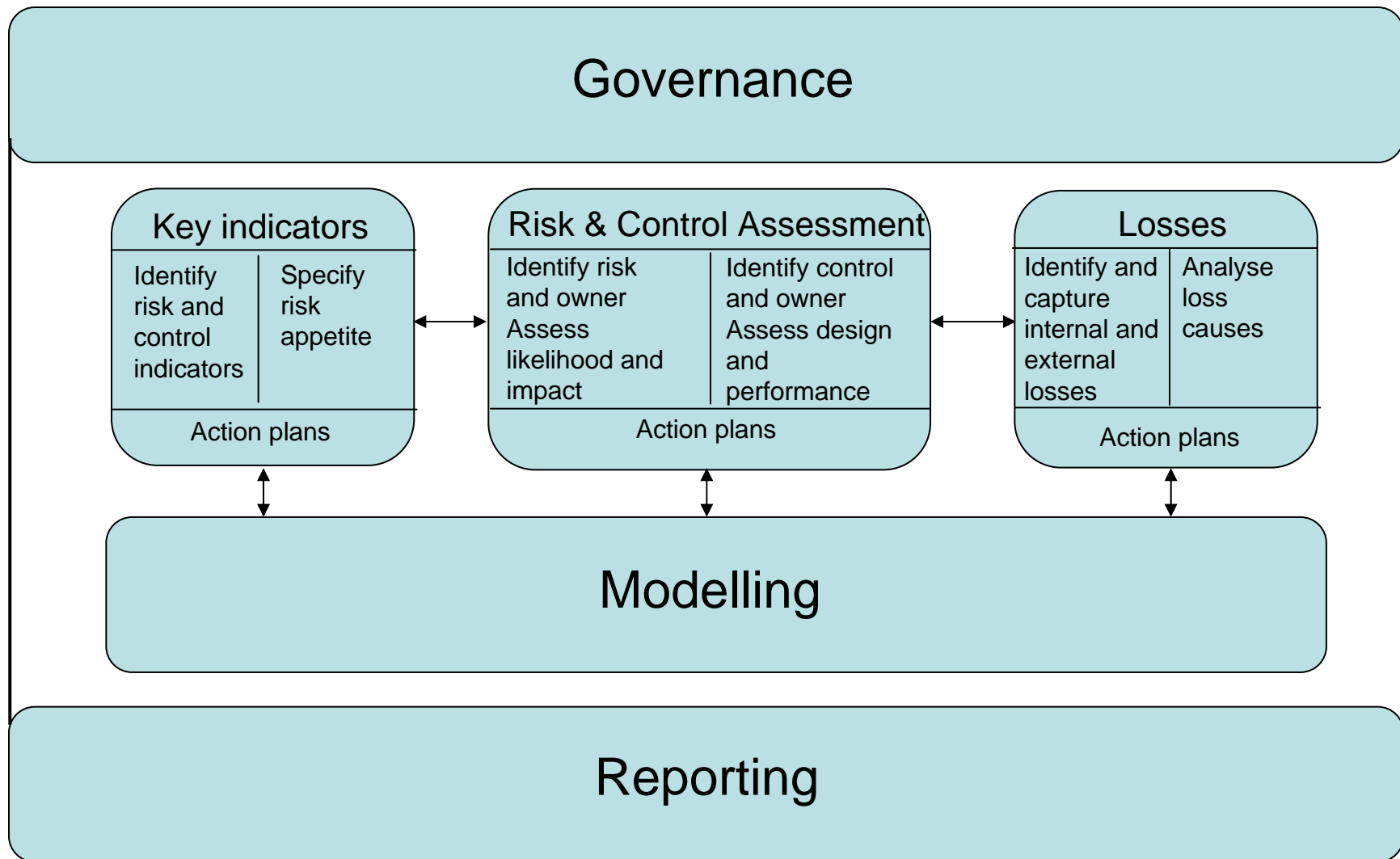
What is excellent ERM?

- Governance
 - Risk ownership at Board / senior management level
 - Established, tried and tested framework
 - Appointed CRO with appropriate authority
- Assessment and aggregation of all risks
 - Relevant metrics for measurement and appraisal
- Risk limits and risk tolerance applied across all business units
- Incorporation of risk into senior management decision process, strategic framework and corporate culture

Key components of ERM

- Governance structure
- Enterprise-wide risk assessment of all risks in all business areas
- Risk appetite (and business optimisation)
- Risk reporting
- Embedding ERM into the firm and its culture

ERM Framework



Governance

- Board/senior management buy-in and sponsorship
- Risk Committee
- Head of Risk
- Risk policy
 - Clear responsibilities and structure
 - Risk ownership clear and unambiguous
- Risk reporting

Where do Risk - and the Head of Risk – sit?

- Relationship to:
 - Board
 - Audit Committee
 - CEO
 - Business line functions
 - Finance
 - Actuaries
 - Audit and compliance
 - Independent validation and quality assurance of framework
 - Reviews adherence to business standards
 - Insurance buyer (i.e. risk transfer)
- Are Risk's roles clear to
 - Risk?
 - The business lines?

The role of the Head of Risk

- Overall risk leadership, vision and direction
- Establishing an ERM framework for all risks
- Developing and reviewing risk management policies (including risk appetite)
- Implementing risk metrics, including early warning indicators
- Allocating risk-based economic capital
- Developing support infrastructure

Implement? Facilitate? Consultant?

Risk policy

- Purpose and scope of policy
- Definitions
 - different risk groups (e.g. insurance/underwriting; market; credit; liquidity; operational)
 - ‘boundary’ issues
 - other definitions i.e. establishing a common risk language
- Risk structure and responsibilities
 - clear and unambiguous ownership of risk and risk policy
- Risk management process
 - deviation from policy – authorised and unauthorised
- Risk appetite
- Ethical and behavioural guidelines

Key components of ERM

- Governance structure
- Enterprise-wide risk assessment of all risks in all business areas
- Risk appetite (and business optimisation)
- Risk reporting
- Embedding ERM into the firm and its culture

Risk management process

- Identification
 - Current risks
 - Use experts to identify emerging risks (e.g. GM food, pollution, climate change etc) for risk and opportunity
 - Prioritise
- Assessment
- Control
- Mitigation

Risk identification and assessment

	Bus. Unit 1	Bus. Unit 2	Bus. Unit 3	Bus. Unit etc.
Insurance risk				
Liquidity risk				
Credit risk				
Market risk				
Operational risk?				

- Business unit or risk type?
- Scenarios (and stress testing)

Insurance risk

- Underwriting risk: life, non-life
 - pricing
- Reserving risk
- Realistic Disaster Scenarios; cat(astrophe) risk
- Methodologies understood
 - 99.5% confidence level?

Liquidity risk

- Need cash to:
 - Meet claims/obligations as they fall due
 - Benefit from opportunities to buy assets
 - Insurers must be counter-cyclical:
 - Buy bonds when interest rates high
 - Buy equities or property when market down
- Insurers need to be cash rich
- But risk assessment required of claims and obligations

Credit risk

- Reinsurers
- Intermediaries
- Investments
 - issuers
 - structured assets, securitisations, special investment vehicles
- Assessment
 - Internal analysis and ratings
 - External ratings

Market risk

- Financial
 - Interest
 - Exchange
- Assets
 - Investments
 - Property
- Assessment
 - VaR etc

Operational risk definition

The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. [BIS, Basel Committee]

Some definitional decisions

NB Basel rider: “This definition includes legal risk, but excludes strategic and reputational risk”

- Legal risk?
- Strategic (or business) risk?
- Reputation risk?

- Where do reputation and other risks fit in to
CAUSE → EVENT → EFFECT or
CAUSE → EFFECT → IMPACT/COST?

Credit risk	Market risk	Liquidity risk	Insurance risk	Group risk	Operational risk
-------------	-------------	----------------	----------------	------------	------------------

Credit risk	Market risk	Liquidity risk	Insurance risk	Group risk	Operational risk
Operational controls	Operational controls	Operational controls	Operational controls	Operational controls	

Is operational risk different from other risks?

	Insurance risk/ Market risk	Operational risk
Is the risk transaction-based?		
Is the risk assumed proactively ?		
Can it be identified from accounting information eg the P&L?		
Can occurrence of the risk (all risk events) be audited?		
Can its financial impact be bounded or limited?		
Can you hold a position in the risk, i.e. can you close out or sell the risk?		

Operational risk assessment

- Risk and control self-assessment
- Loss event data
 - Internal
 - External (pooled; public)
- [Key] [risk] indicators

Risk self-assessment

- A matrix to assess frequency/probability and severity/impact.
- Involves some degree of scoring
 - traffic lights (red, amber, green) or H,M,L
 - larger number of grades (ideally min. 4)
 - mathematical extrapolation.

But there's a missing ingredient . . .

Frequency and severity – traditional view of operational risk

High (3) Frequency	3	6	9
Med (2)	2	4	6
Low (1)	1	2	3
	Low (1) Severity	Med (2)	High (3)

Control risk self-assessment

- Two assessments are required
 - Assuming controls work (net)
 - Assuming controls fail (gross)
- The final result will provide
 - A league table of risk exposures, which will drive management action and provide the basis for cost-benefit evaluations of new controls
 - A risk map for senior management
 - Provides feeds to internal and external auditors regarding the effectiveness or weaknesses in controls

Frequency and severity – traditional view of operational risk

High (3) Frequency	3	6	9
Med (2)	2	4	6
Low (1)	1	2	3
	Low (1) Severity	Med (2)	High (3)

Frequency and severity - modern operational risk management

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

Loss event data – what is included?

- Reporting threshold
- Near misses
- Indirect costs and costs to fix
- Offsets and gains, i.e. why just losses and costs?
- “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 . . .

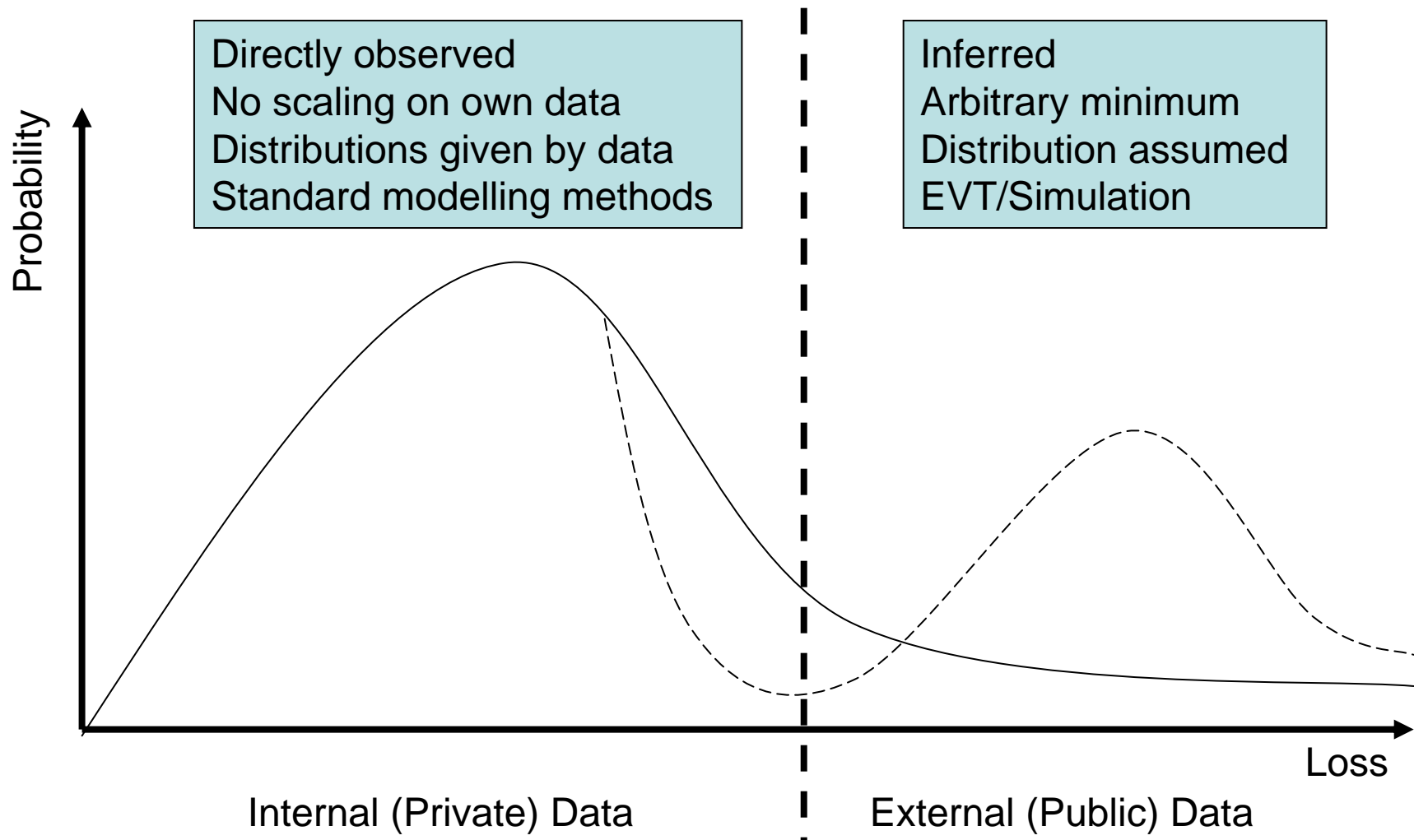
- Focus management attention on areas of activity that are giving rise to losses
- Validate risk self-assessments, scenario analysis, key risk indicators and capital allocation.
- It is therefore extremely useful as *information*.

External data is similar – only more so . . .

External loss event data – more health warnings

- Pooled, e.g. ABI, ORX, BBA GOLD
 - All the concerns of internal data
 - As with internal data, its construction and nature will depend on the purpose for which it is gathered
 - Different risk, control and reporting cultures
 - Exclusions (e.g. legal, insurance settlements)
 - Scaling?
- Public data, e.g. Aon (claims), Willis (for “clients”), FitchRisk
- External data
 - provide *information*
 - validate and enhance self-assessment
 - enhance OR management rather than measure “severe” losses

The Tail Problem



What is a key risk indicator (KRI)? [1]

- A KRI:
 - is a warning light of future risk exposure
 - measures trends
 - is *not* a predictor of the future
 - identifies factors which have not yet become events

What is a KRI? [2]

- KRIs should be meaningful drivers of risk (ie related to *causal* factors)
- With a true risk indicator, there must be a relationship between the indicator and loss severity and/or loss frequency
- KRIs enable early detection and management of unacceptable risk in each function or process against predefined tolerance levels i.e. triggers and thresholds.
- Breaking a KRI trigger or threshold must lead to ***action***

KRI examples (1)

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

KRI examples (2)

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

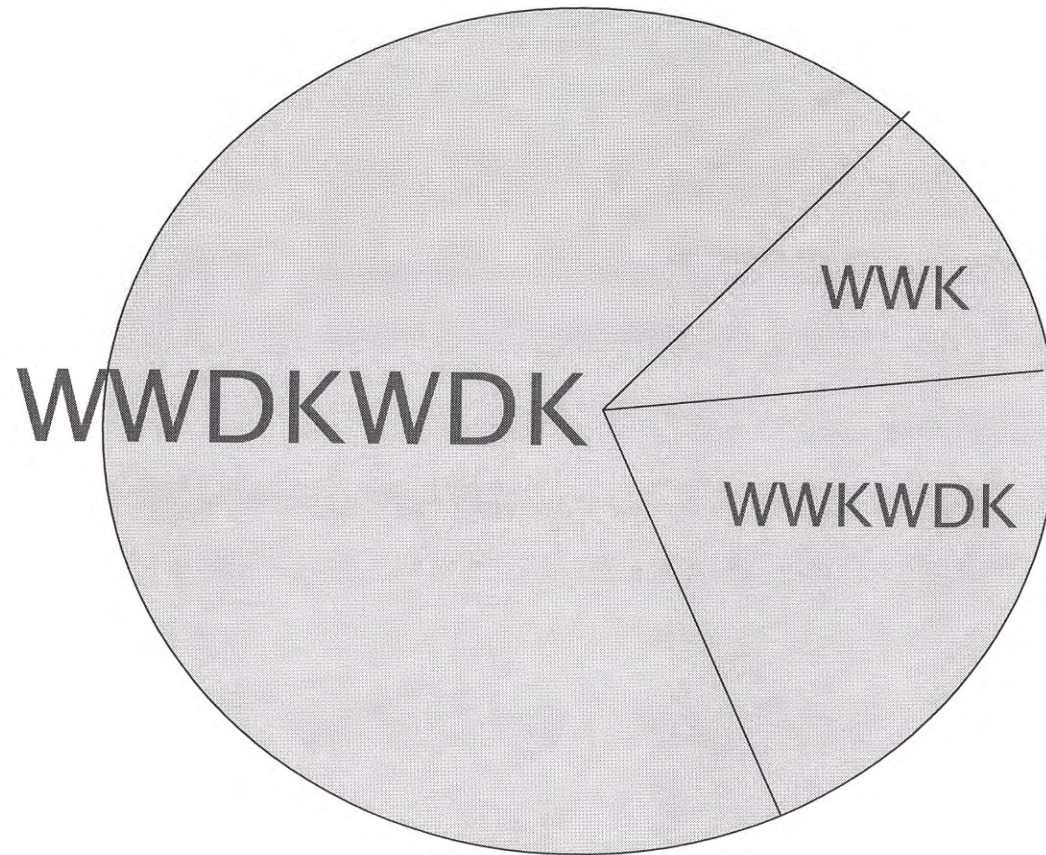
Risk indicators - an Audit Committee perspective

NB almost all Yes/No

[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

An Uncertain World



not forgetting **WWDKWK**

Scenario analysis

- Scenarios are about assessing tail events i.e. the 1 in 200 (?) year event
- Tail events generally result from:
 - Several controllable small things going wrong
 - Uncontrollable external catastrophe(s)
 - A combination of the above
- Scenarios should represent combined events and attempt to cover insurance risk, market risk and broader (operational?) risks to the firm

e.g.

Combined scenarios – examples

- 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.

[Extracted from Lloyd's ICA Guidance 2007]

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)

Key components of ERM

- Governance structure
- Enterprise-wide risk assessment of all risks in all business areas
- Risk appetite (and business optimisation)
- Risk reporting
- Embedding ERM into the firm and its culture

Risk appetite definition

The amount that a firm is willing to risk

(for a given risk-reward ratio)

Risk appetite

- Insurance/underwriting risk
 - Realistic Disaster Scenarios/Willingness to Lose
 - Policy Limits
 - Aggregates
 - Underwriting policies/protocols
- Market risk
 - Position and deal limits by trader, currency etc
- Credit risk
 - Limits
 - Ratings
- Operational risk? Remember the 'What's different about OR' slide: can you put a limit on operational risk?

How to Measure Risk Appetite (1)

Each of the four major processes can be used:

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

How to Measure Risk Appetite (2)

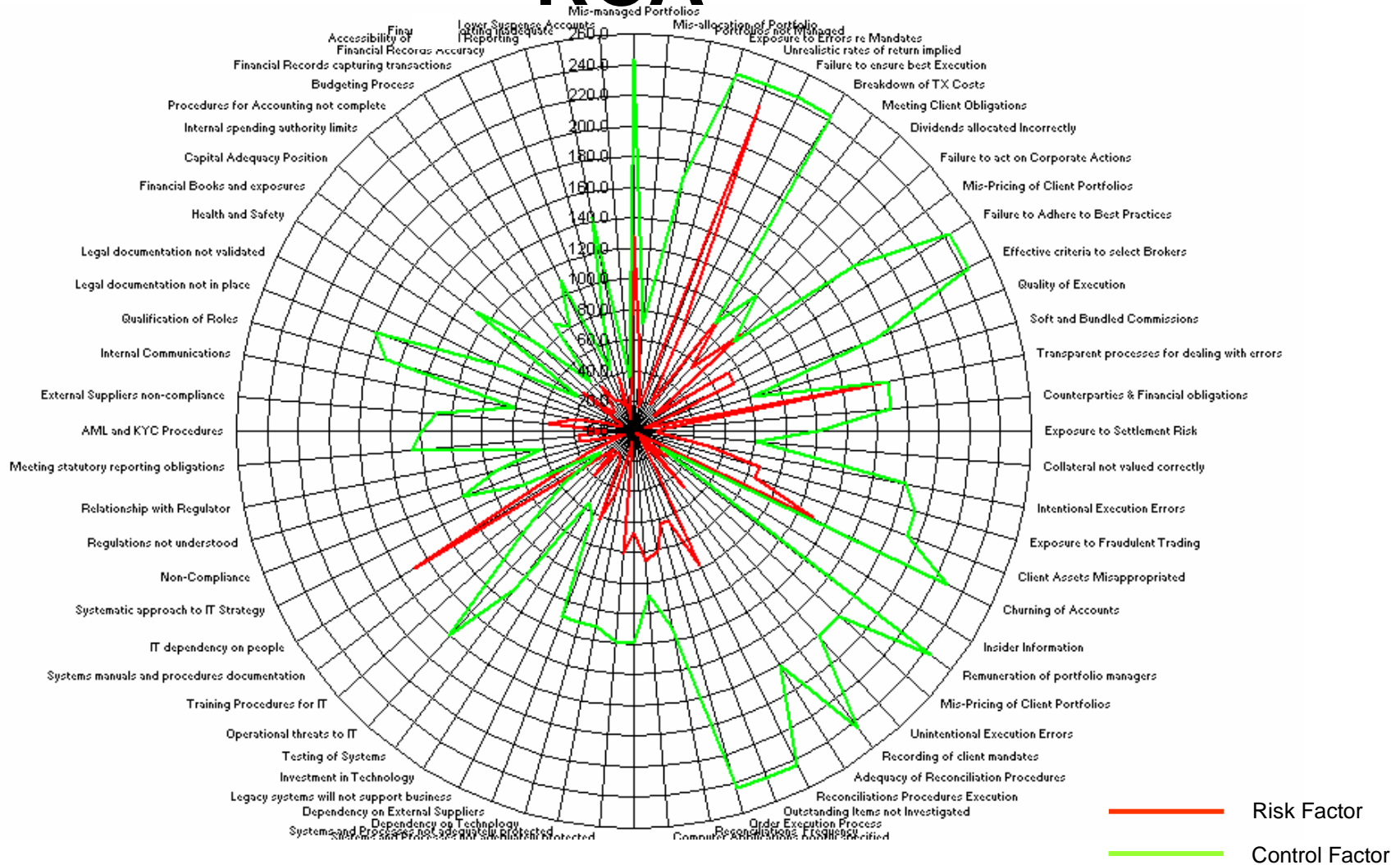
- Expected loss
 - Easy but you probably already know it
- Unexpected loss
 - More difficult
 - Mathematical modelling
 - Explanation of concepts to senior management

Risk appetite and business optimisation

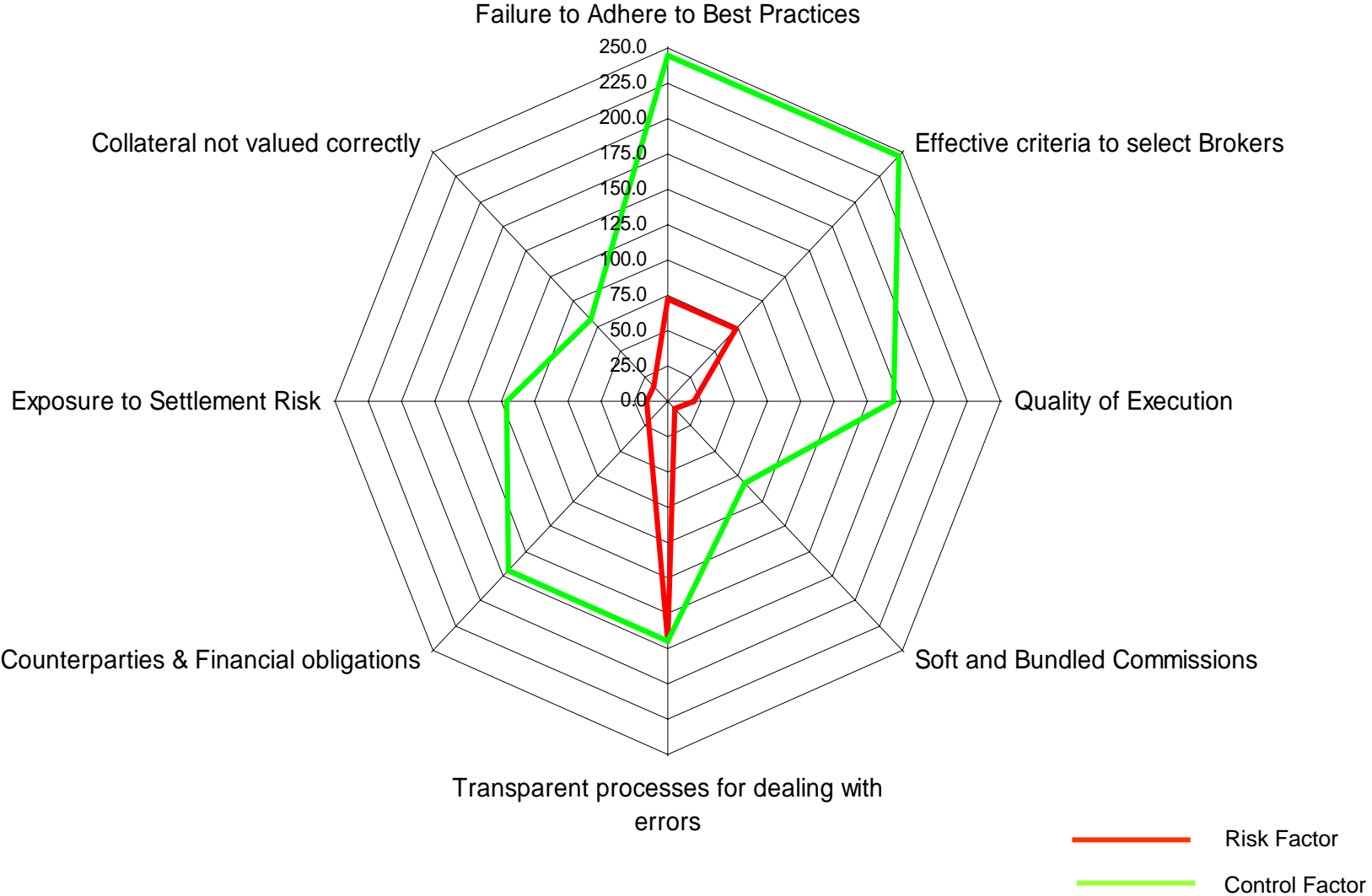
Six examples using:

- RCA
- RCA annual loss
- Indicators
- Number of losses
- Value of losses
- Value of controls

RCA



Organisational Risk & Control Factors



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

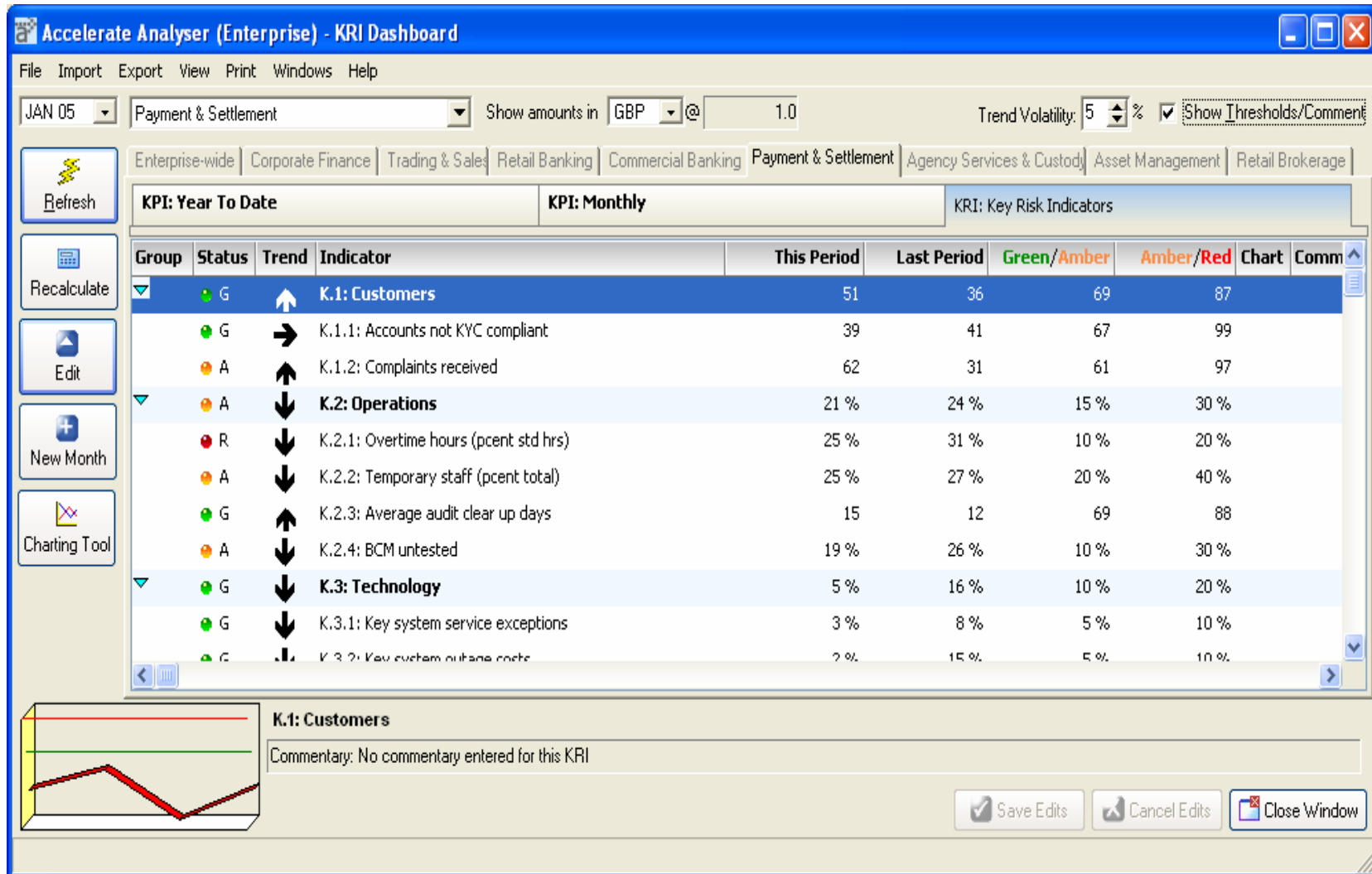
Annual Frequency

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

Indicators



Number of Losses

Accelerate ECO (Economic Capital Optimiser)

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

View

- LDA Internal
- LDA External
- CRSA
- Combined (Classical)

View in: full

Total Capital Charge: 282,616,256

Selected Cell

Corporate Finance
Internal fraud

	LDA Internal	LDA External	CRSA	Combined
Percentage Weight:	50	0	50	Classical
<input checked="" type="radio"/> Number of Loss Events:	44	0	45	44
<input type="radio"/> Mean Severity of Losses:	80,658	0	127,805	104,231
<input type="radio"/> Std Deviation of Losses:	104,540	0	169,046	140,544

↑ 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
Corporate Finance	44	12	95	22	77	44	63
Trading & Sales	24	12	39	11	74	30	10
Retail Banking	22	79	21	46	38	10	14
Commercial Banking	35	10	35	10	18	35	3
Payment & Settlement	25	59	89	32	35	9	47
Agency Services	41	54	46	36	94	1	94
Asset Management	20	72	85	77	56	77	85
Retail Brokerage	56	16	27	98	55	97	46

Value of 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
								
Corporate Finance	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
TOTAL	41,898	53,579	42,837	29,000	36,127	39,752	39,597	282,590

Quit

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
TOTALS	145,530	43,233		102,297

Key components of ERM

- Governance structure
- Enterprise-wide risk assessment of all risks in all business areas
- Risk appetite (and business optimisation)
- Risk reporting
- Embedding ERM into the firm and its culture

Other elements which contribute to the overall picture

- Groupwide risk issues – main company concerns
- Project risk assessment
- Yes/No issues
- Near misses
- Capital calculation
- Scorecards for overall risk and risk process effectiveness

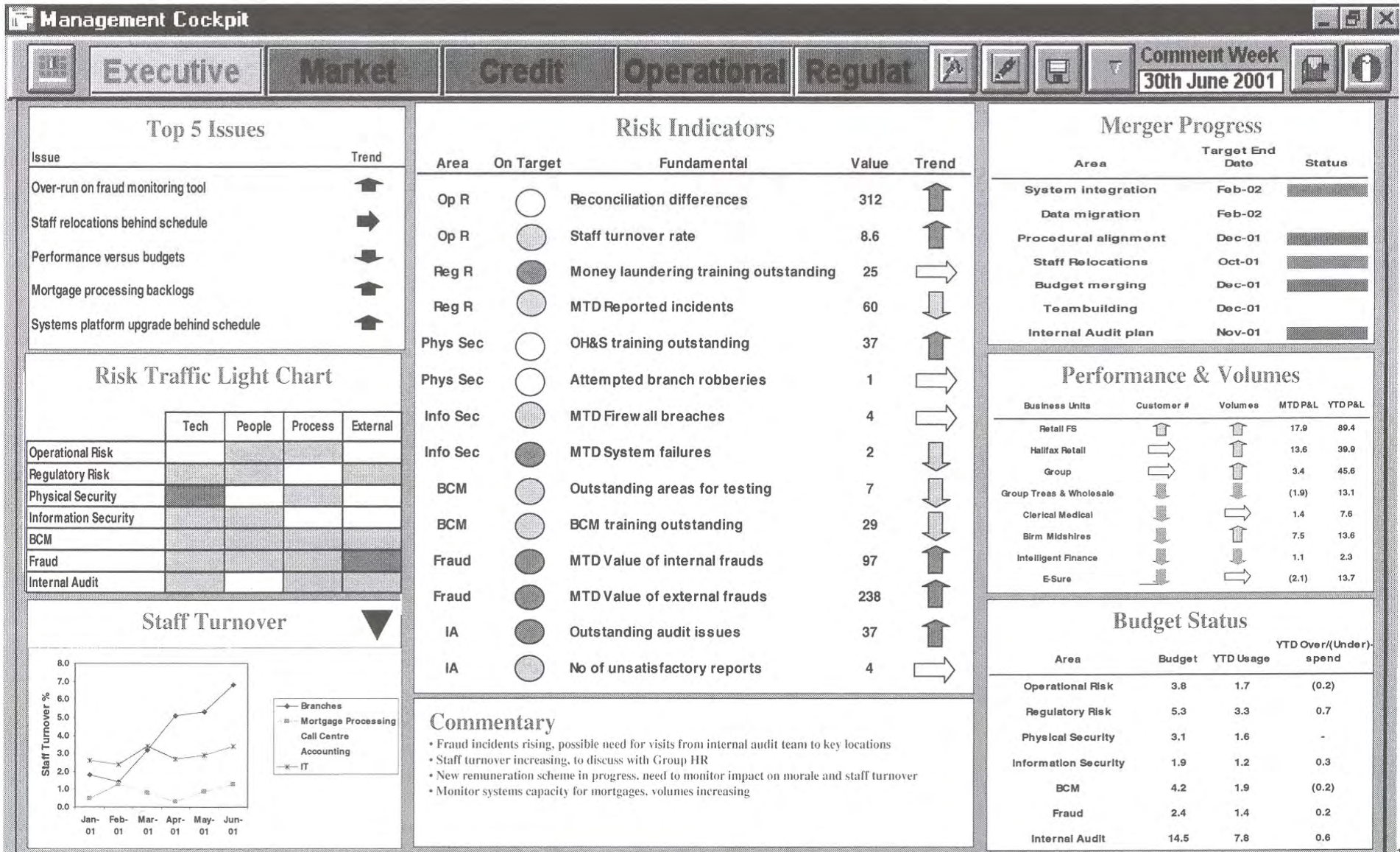
Risk effectiveness (subjective assessment)

Factors Accessed	Related Questions	Business 1	Business 2	Business 3	Business 4
Responsibility assigned and suitable skills available	<ul style="list-style-type: none"> - Appropriate/required resources in place to provide advice/guidance/direction? - Business access to appropriate expertise? 	8 →	3 ←	7 →	8 →
Governance Direction / Oversight	<ul style="list-style-type: none"> - Snr Mgt direction and oversight? - Regular progress and issue reporting? - Informed risk debate and formal risk acceptance? 	8 →	6 ↔	7 →	8 →
Policy Implementation	<ul style="list-style-type: none"> - Has a policy gap analysis been completed? - Is there an action plan defined for addressing the gaps? - Has the action plan been implemented? 	8 →	6 ←	6 →	9 →
Risk Identification and Assessment	<ul style="list-style-type: none"> - Are risk assessments on projects performed? - Are major risks identified in ORP? - is the process robust and subject to challenge? 	6 →	5 ←	7 →	8 →
Risk Awareness	<ul style="list-style-type: none"> - Implementation of a formal awareness programme ? - Effectiveness measured & continuous awareness reinforced? 	7 →	5 ←	6 →	9 →
Risk Measurement and Reporting	<ul style="list-style-type: none"> - Are KRI's defined, monitored and reported? - Are major risks identified and reported? - Are events reported (including external?) 	7 →	5 ↔	6 →	6 →
Other					
Additional Comments					

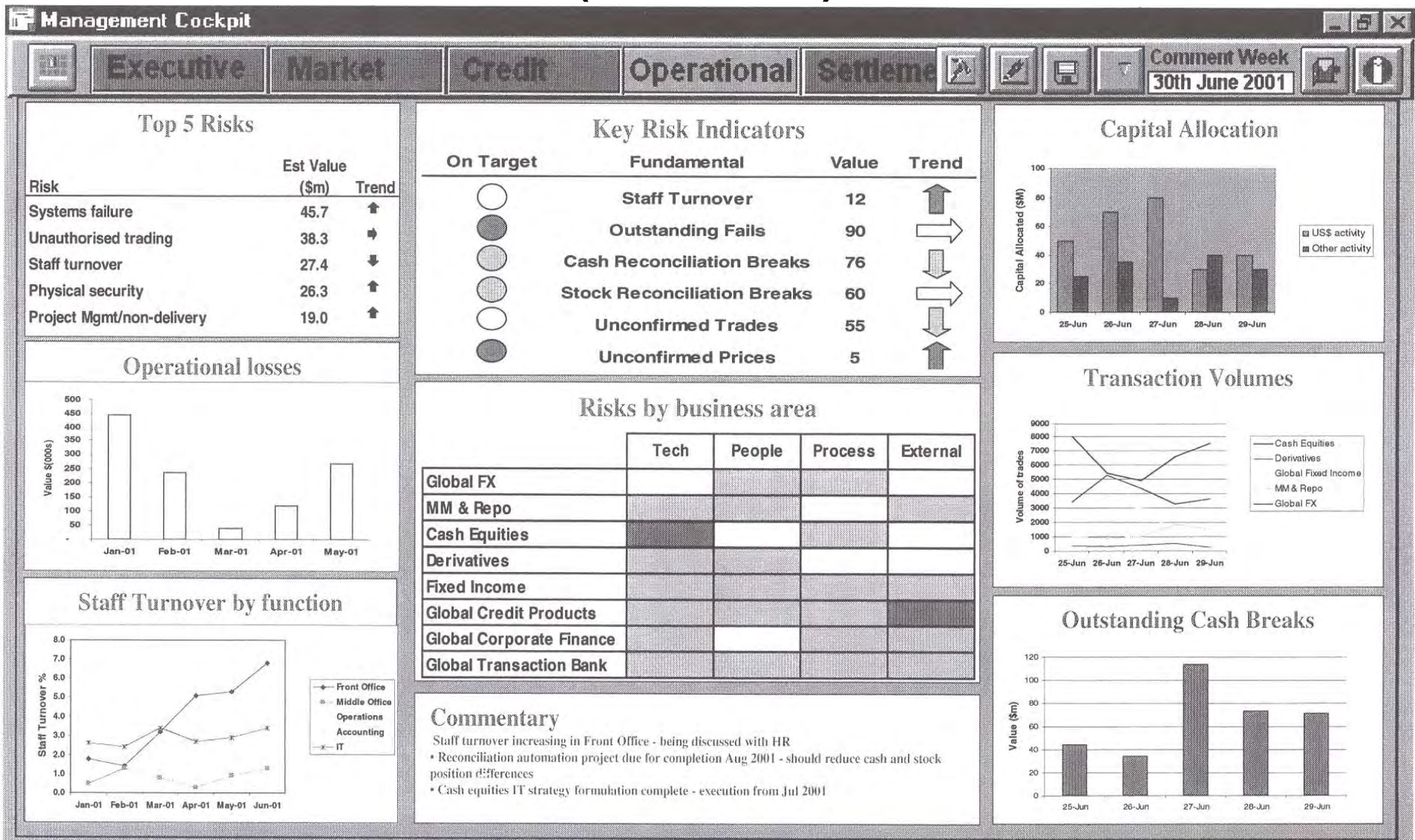
↔	No Change
→	Improving
←	Deteriorating

Average 6.8 (5.4)

Executive dashboard (level 1)

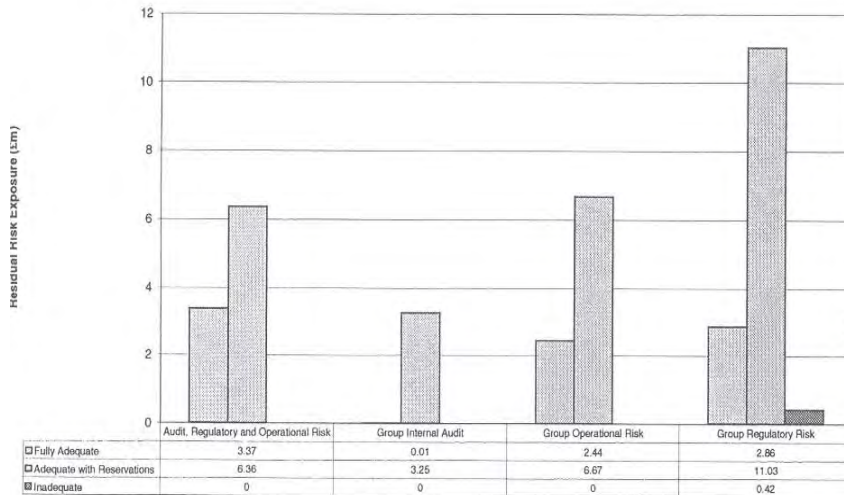


Operational dashboard (level 2)

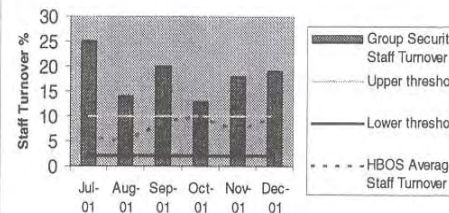


Core systems report (level 3)

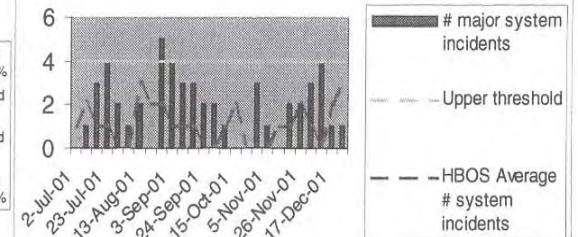
Residual Risk Exposure by Control Adequacy - Audit, Regulatory and Operational Risk as at 30th June 2003



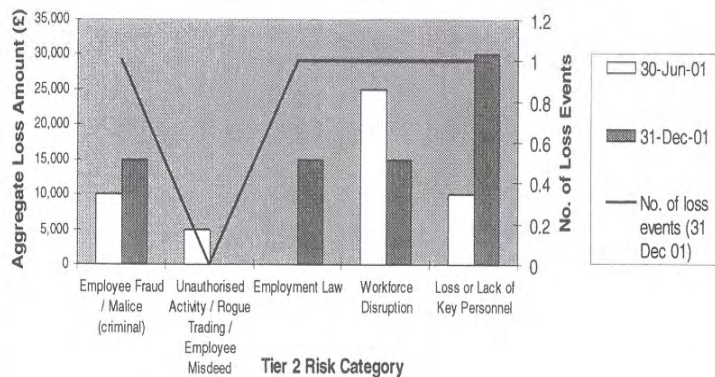
Group Security - Staff Turnover %



Group Security - Number of Major System Incidents



Loss Events by Tier 2 Risk Category



Mandatory Fields indicated by (*)				
*Organisation Unit	Audit, Regulatory and Operational Risk			
Risk Record				
*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.			
Risk Record - Details				
* 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 ORWP		Ineffective SLA with service providers, leading to lack of control and influence over resourcing decisions made by internal or external service providers		

Key components of ERM

- Governance structure
- Enterprise-wide risk assessment of all risks in all business areas
- Risk appetite (and business optimisation)
- Risk reporting
- Embedding ERM into the firm and its culture

Embedding risk

- Risk strategy – know what questions to ask; what battles to fight and win
- Organisation – make sure Risk has the right authorities and the right people are involved in decisions
- Processes – can they take decisions
- Information – to support the decision makers
- Systems – invest in the infrastructure

An ERM culture

- An ERM culture is what you get after a successful implementation of a framework, where everybody in the organisation is aware about risk. It's in the corporate bloodstream or DNA.
- ERM should be part of any business decision by providing a basis for risk assessment, including changes in strategy, new products/classes, re-engineering.
- The tone will come from the top.
- A strong risk culture is a pre-requisite for balanced risk-taking

The good ship Culture

- Build the boat
 - Define CRO's role
 - Formalise CRO's office
 - Create senior level focus on risk issues
- Get people aboard
 - On-going discussions of risk and capital and emerging issues
 - Group-wide project
 - Peer review for risk diagnostic
- Set sail
 - Yearly CRO conference
 - Senior level risk seminar
 - Active participation of CRO and staff in local risk committees

Summary

Enterprise-wide risk management is about managing all risks. It is not about managing all risks in the same way.

Nor is it about avoiding risks but about improving the health of the organisation.

If it is done well, the benefits are considerable.

Adding value through ERM

- Strengthening risk culture and awareness
 - Buy-in from Board, senior management – a cohesive organisation
 - Risk policy; minimum standards; risk assessment
 - Risk adequate organisation
- Supporting value creation and decision-making
 - Reduce surprises and losses
 - Risk/reward balance, leading to increased revenues
 - High quality information about risks and opportunities
 - Enhance risk response decisions
 - Risk tolerance and appetite, aligned to strategy
 - Emerging risks management
- Protecting the capital base
 - Ensure adequate risk oversight
 - Internal risk capital and stress tests
- Survival of the species

John Thirlwell

Tel: +44 (0)20 8386 8019

E-mail: info@johnthirlwell.co.uk