Risk, governance and compliance

John Thirlwell

Sliema, Malta, 6 March 2009

- What do we mean by risk?
- Risk and corporate governance
- Classes of risk
- Risk management v risk measurement
- The risk management toolkit

What do we mean by risk?

- . . .something that might happen and its effect(s) on the achievement of objectives. *BS31100 Code of Practice for Risk Management*
- . . . the chance of something happening that will impact objectives . . . *AS/NZS 4360:2004 (Australian/New Zealand(?) Standard from ASI)*
- Those objectives can be sales, profits, market share or something other. They will usually result in financial loss, but not necessarily so.
- Operational risk: The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. = business risk?

CAUSE → EVENT → EFFECT

What is Enterprise-wide Risk Management (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 do we mean by risk?
- **Risk and corporate governance**
- Classes of risk
- Risk management v risk measurement
- The risk management toolkit

Where do Risk - and the Head of Risk/Chief Risk Officer – sit?

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

Risk policy

- Purpose and scope of policy – overall objectives
- 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
  - principal sources of risk
  - deviation from policy – authorised and unauthorised
  - measurement, management and reporting
- Risk appetite and risk tolerance
- Ethical and behavioural guidelines

The 3 lines of defence

1	Business operations	• Established risk and control environment • Ownership
2	Oversight functions: Finance, Quality, HR, Compliance and Risk	• Strategic management • Policy and procedure setting • Functional oversight
3	Independent assurance: Internal audit, external audit, other independent assurance providers	• Provide independent challenge and assurance

The role of the Chief Risk Officer

- 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?

What is excellent ERM?

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

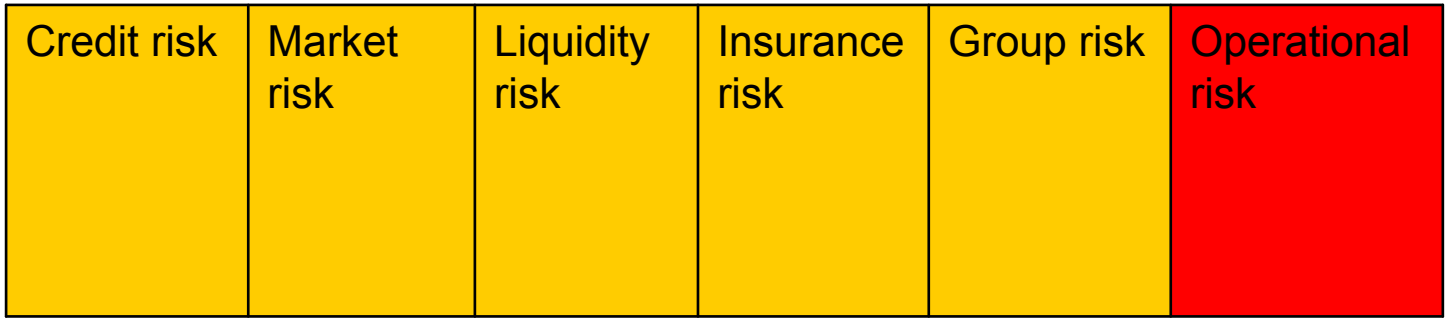
The Board/NED/Audit Committee perspective

- Is there a clear set of risk management objectives?
- Does the executive take risk management seriously?
- Where does ownership for risk management reside?
- Is there a structure for strong oversight and challenge?
- Is general risk awareness visible? i.e is there a strong risk culture?

- What do we mean by risk?
- Risk and corporate governance
- **Classes of risk**
- Risk management v risk measurement
- The risk management toolkit

Classes of risk

- Credit
- Market
- Liquidity
- 3rd party dependencies
  - In, e.g. suppliers
  - Out, e.g.agents
- Operational
- Reputation
- Strategic


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	

Some other risks

- Strategic and business risk – should they be included within operational risk?
- Where does reputation risk fit in?

Reputation risk

- Reputation
  - takes years/decades to build and moments to lose
  - is the largest asset in value and is crystallised when a business is sold
  - is a valuable barrier to entry
- Reputation risk
  - is almost always a *consequence* of events caused by other risk types, but OR is probably the main source
  - can result from competitors' activity
- Reputation risk management = management. Good management will accrue reputation.
- Management's response to a crisis will probably affect reputation more than the nature of the crisis itself.
- Is there an optimum reputation?

Is operational risk different from other risks?

	Credit/Insurance/Market/Liquidity 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?		

- What do we mean by risk?
- Risk and corporate governance
- Classes of risk
- **Risk management v risk measurement**
- The risk management toolkit

- Can you manage what you can't measure?
- In other words, is measurement central to management?
- What should you be measuring?

  CAUSE → EVENT → EFFECT

  or, if you prefer,

  CAUSE → EFFECT → IMPACT/COST
- Hard and soft measures
- Historic (risk) and forward-looking (risk exposure) measures

Measures of risk

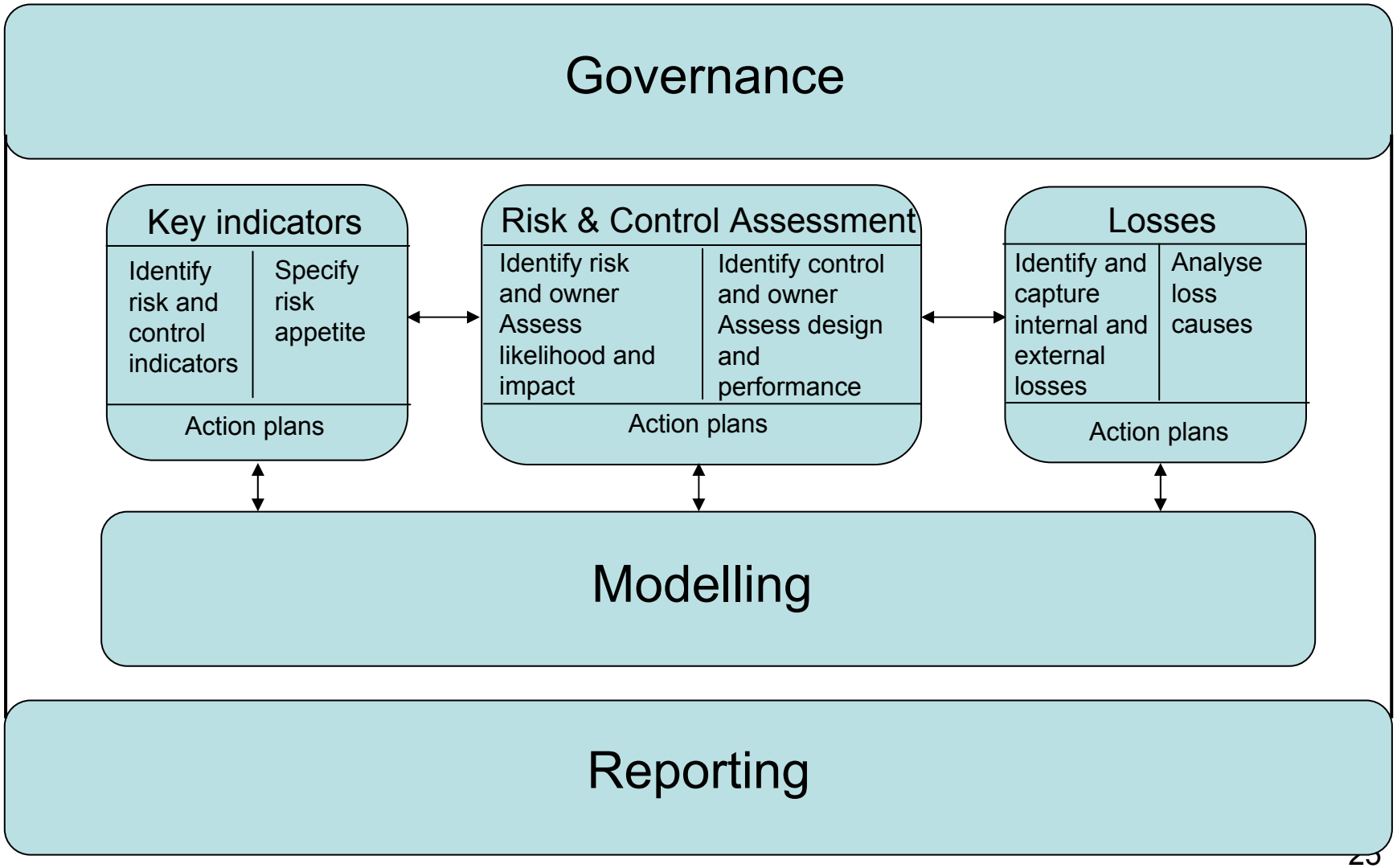
- Losses or costs
- Assessments
- Indicators

What can you do about risk?

- Control (to within risk appetite)
- Contain (after it has happened)
- Accept

- What do we mean by risk?
- Risk and corporate governance
- Classes of risk
- Risk management v risk measurement
- **The risk management toolkit**

ERM Framework



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

Risk 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.

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

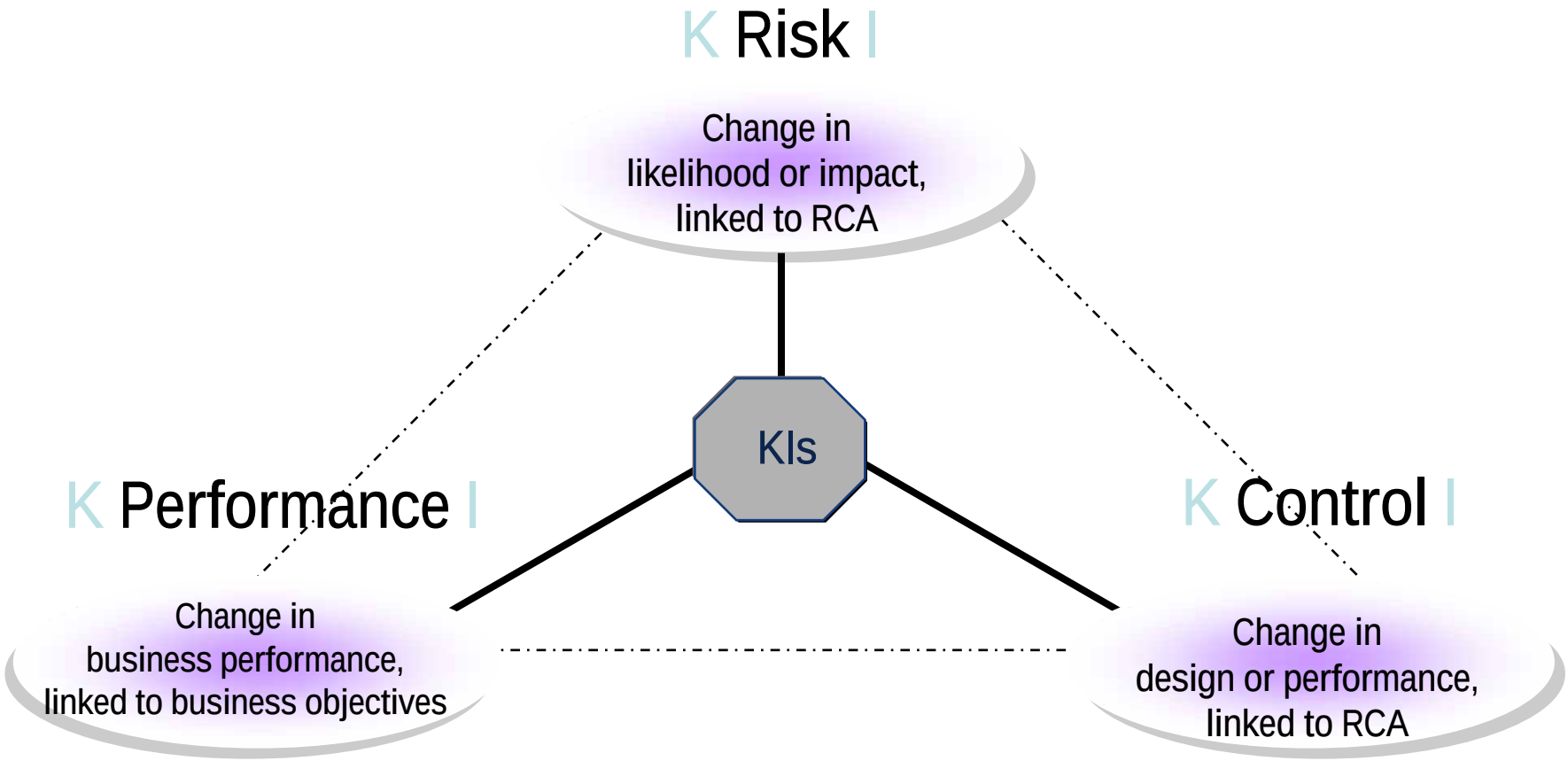
High (3) Frequency		n/a	n/a
Med (2)			n/a
Low (1)			
	Low (1) Severity	Med (2)	High (3)

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

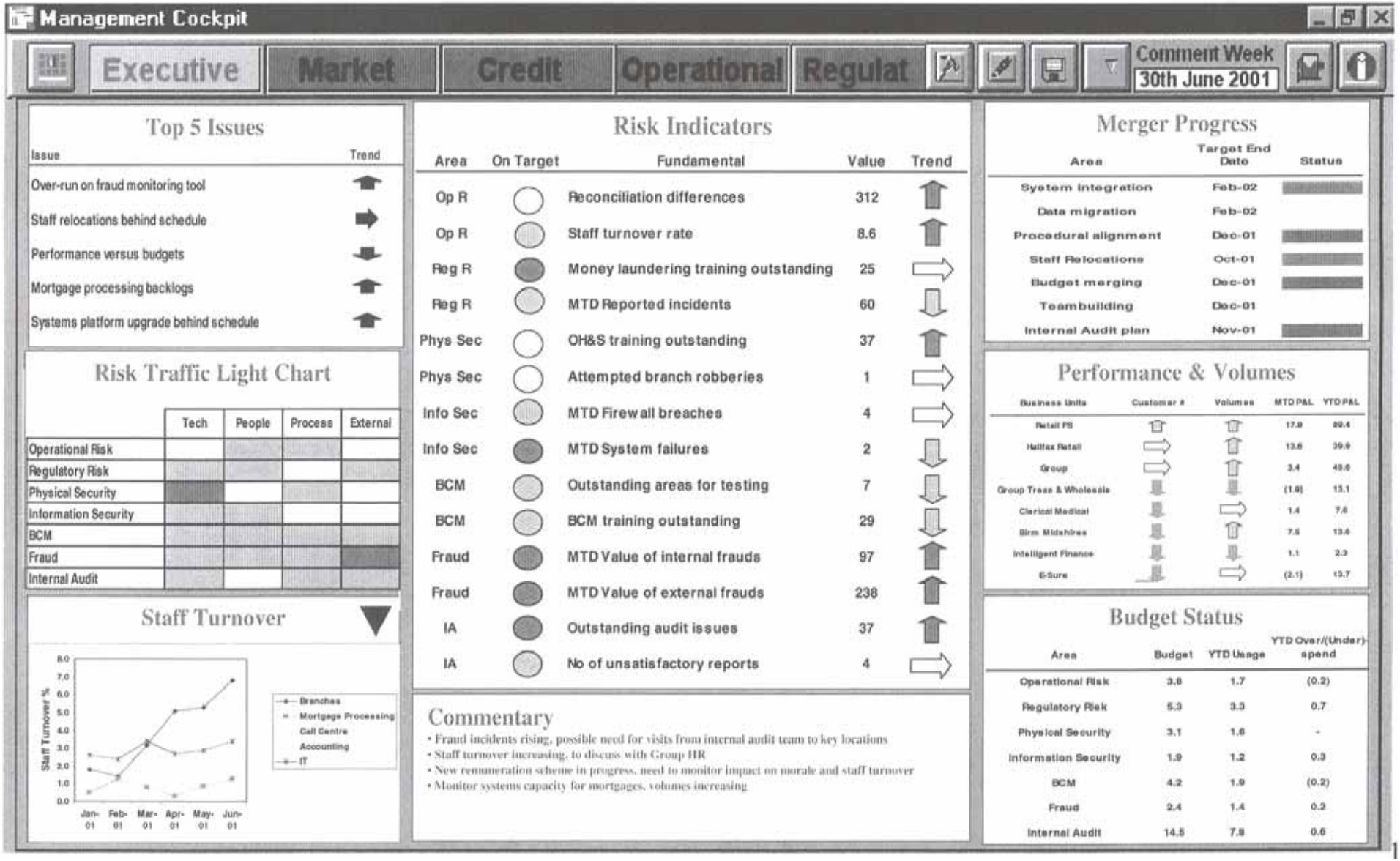
Indicators


K Risk I
Change in likelihood or impact, linked to RCA
KIs
K Performance I
K Control I
Change in business performance, linked to business objectives
Change in design or performance, linked to RCA

Other elements which contribute to the overall picture

- Groupwide risk issues – main company concerns
- Project risk assessment
- Yes/No issues
- Near misses
- Capital calculation

Executive dashboard (level 1)



John Thirlwell

Tel: +44 (0)20 8386 8019

E-mail: info@johnthirlwell.co.uk