Good and Bad Practices for Risk and Control Monitoring

Disclaimer

- Your speaker is a Fellow of the Institute of Directors, as well as the Chief Executive of the Risk*Business* Group.
- The views expressed in this presentation are the sole responsibility of the presenter and do not and can not be construed as representing the view of either the Institute of Operational Risk or of the Risk*Business* Group.

What is a KRI?

- Basically, whatever you want it to be!
  - It's a metric, a piece of data or information.
  - It only has value to those who can use it.
  - Generically, from a risk management perspective, it provides an indication about risk exposure at a point in time.
  - There is no difference between KRIs, KPIs and KCIs – it all depends on the source and use of the information.

Who owns indicators?

- Who decides which indicators to monitor?
- Who decides how the indicator values are calculated?
- Who decides who receives indicator reports and when they receive them?
- Who decides when to escalate an indicator submission?
- Who decides to discontinue using a specific indicator?

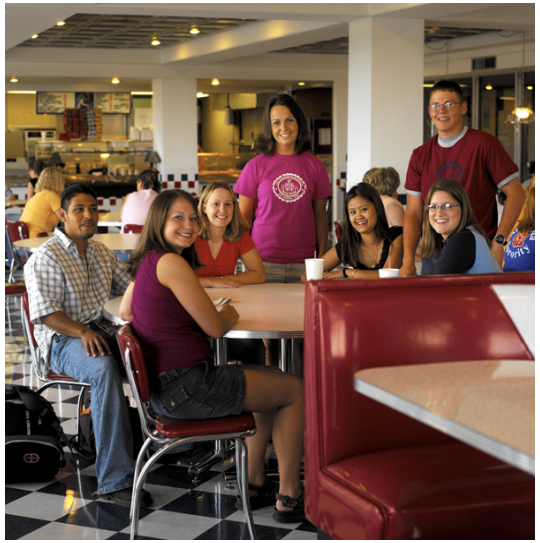
Roles in the indicator process

Providers

Producers

Risk Management

Consumers



Observers

THE INSTITUTE OF OPERATIONAL RISK

Which risks and controls should be monitored?

- The academic answer is “all of them”.
- The regulator’s answer is whichever ones you think are important.
- The risk practitioner’s answer is “key” risks and controls.
- The business’ view is as few as possible, we don’t have time for this garbage!

- So how many indicators do we need?
- As many as you can without causing undue business disruption – look for “automatic indicators”.

Defining leading and lagging indicators

- There is no such thing as a “predictive indicator”!
- Indicators are bits of data – to be data, something has happened to generate that data, indicators are thus historical measures.
- Any array of data will reflect historical trends. All things being equal, trends can be extrapolated into the future. But, operational risk is all about the uncertainty of people, hence do not assume that trends predict the future.
- Indicators provide information on the past (lagging) and the present (current). A current exposure, particularly if increasing in magnitude, may indicate future (leading) problems.

Defining thresholds for escalation

- Thresholds are essentially pre-defined limits which, when the value of an indicator reaches that level, generates warnings or alerts.
- Different types of alerts:
  - Touch
  - Repetitive touch
  - Percentile breach
  - Trend threshold
- Thresholds should never be absolute; they need to address cycles and correlations.
- Ideally, they escalate in accordance with the severity of the issue they represent.

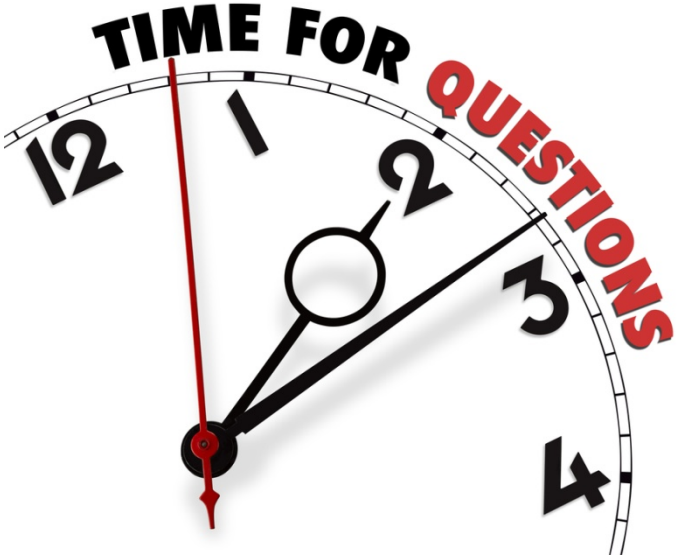
Threshold issues

- Never start with a “big bang” – management will be confused if they suddenly start receiving numerous “alerts” and “warnings”.
- Start with high-level thresholds and fine tune them over time – what is the correct level for any metric?
- Use layered structures so that increasing levels of seniority receive warnings when appropriate – and the “worker-bees” do not get a surprise.
- Revise thresholds from time to time.

In summary……

- There is no such thing as a global set of “top 10” indicators which everyone should monitor.
- Excluding composite or index-based metrics, indicators are not in of themselves predictive.
- A good indicator programme will involve a large number of players.
- Your risk profile is constantly changing, causal drivers continuously morph into different impact chains – the indicator set being monitored should thus not be set in stone.
- Revise thresholds regularly, monitor continuously.
- Don’t expect instant gratification – the benefits of the indicator programme will take time to manifest themselves.

Questions and Comments



- ***Contact Details:***
- Mike Finlay, Chief Executive, Risk*Business*
  - Telephone : +44 7721 969 224
  - E-mail : mike.finlay@riskbusiness.com
  - URL : www.riskbusiness.com and www.ior-institute.org