Some quotes:

Commercial sense – resetting the tolerance for risk

‘The Board defines the organisation’s risk tolerance’

‘When I started here our 20-page risk register only had 4 of the 7 big risks’ – ‘You were lucky to have over half’

‘By following our six principles, <including clear risk tolerance>, organisations can move from… process to one which supports efficient effective delivery’

‘Numbers were understated nearly 50% because…’

‘Governments of all colours have struggled to procure and manage big new projects’
Today

Scene - Setting - Generic

- Public Sector

Managing Public Money
What is wrong with how Boards identify and manage risks

Why worry about the headlights working when you’re in this position?

Black Swan events – what are the chances of a destructive solar storm? Often higher than some events given much more attention

Why are there no tools or competencies for big or strategic risks?

Goldman/JP Morgan v Lehman/HBOS

Who had the best Risk Registers before the recent financial crisis?
Issues in Risk Management (for Boards to consider)

How do you sort out the wood from the trees?
How do you manage for black swan events?
How do you devise a truly effective Board level risk register?
How do you manage and handle strategic risk?
How do you better quantify?
Three key lessons

1. It would be nice to predict
2. Heatmaps are great at operational level but don’t really work at Board level
3. Failure of an organisation is often caused by contagion
The problem with heatmaps (sometimes known as probability/impact diagrams) at strategic Board level

Here is a heatmap (taken from page 25 of the Government’s Orange book)
So... are there any lessons from maths/statistics that can help?

But first.... Public sector
What is Public Sector?

Q: What is strategic in different parts of public sector?
Q: How many reference works on risk in Government?
Q: How do you measure success and failure for each element?
Attitude to risk of Chief Risk Officers - Sector

App 3 Figure 4. Risk Type distribution across industry sector

Source IRM Culture Survey 2012
## Complementary ways of looking at risk

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Board responsibility</td>
<td>(The 6 ‘What’)</td>
<td>• Board’s strategic guidance should permeate</td>
</tr>
<tr>
<td>• Better risk taking</td>
<td>• Engaged Board to focus on</td>
<td>• Need for top-down and bottom-up</td>
</tr>
<tr>
<td>• Committee structure clarity</td>
<td>• managing the things that matter</td>
<td>• Board defines Risk Tolerance</td>
</tr>
<tr>
<td>• Risk appetite/tolerance</td>
<td>• Clear risk tolerance →</td>
<td>• Board considers likelihood of outcomes</td>
</tr>
<tr>
<td>• Board focus on key risks</td>
<td>proportionate risk response</td>
<td>beyond tolerance and decides which risks</td>
</tr>
<tr>
<td>• Reputational risks</td>
<td>• Have clear</td>
<td>matter</td>
</tr>
<tr>
<td>• New approaches</td>
<td>ownership/accountability for risks</td>
<td>• Each organisation should decide what works</td>
</tr>
<tr>
<td>• Net risk is dangerous</td>
<td>• Quality information</td>
<td>best for them.</td>
</tr>
<tr>
<td>• MI</td>
<td>• Evaluation and costing</td>
<td>• QA of models</td>
</tr>
<tr>
<td>• Transparency, accountability, reporting lines</td>
<td>• Implement lessons learned</td>
<td></td>
</tr>
<tr>
<td>• Role of assurance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Corporate culture</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Better reporting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Update Turnbull</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1010
**Expected Sharman recommendations**

To enhance behaviours:

An integrated assessment of risks that may threaten survival to inform both going concern (financial) and narrative reporting

Narrative reporting about such risks integrated with business model, strategy and principal risks

An enhanced role for auditors

* Applicable to private sector companies, with simplified approach for SMEs, but could well become “best practice” more generally
Managing public money
Box A4.3A: Outline of the risk management cycle

1 The Board defines the organisation’s risk tolerance.

2 The organisation identifies and categories its risks.

3 The organisation assesses the risks identified: how likely their possible impact, identifying which are beyond tolerance and when.

4 The Board scans the horizon for any remote overlooked risks.

5 The Board decides which risks matter and what action should be taken, if any.

6 Downward delegation of management, coupled with upward reporting of risks through the organisation enables the Board to track performance

7 Using this feedback, the Board takes a rounded overview, and may adjust decisions eg on tolerance or on response.

8 Back to step 1 and iterate as the Board chooses.

Source: Managing Public Money July 2013
<table>
<thead>
<tr>
<th>PRINCIPLE</th>
<th>REVIEW PROCESS</th>
<th>ALIGNMENT</th>
<th>REPORTING FORMAT</th>
<th>REPORTING FREQUENCY</th>
<th>FOCUS OF BOARD DISCUSSION</th>
<th>CRISIS MANAGEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Who owns strategy</td>
<td>• Questionnaire</td>
<td>• Top down</td>
<td>• Specimen to follow</td>
<td>• Every Board meeting</td>
<td>• Horizon scan new causes</td>
<td>• Can be incredibly efficient &amp; effective</td>
</tr>
<tr>
<td>• Who owns strategic risk</td>
<td>• Review strategy/ Business Plan</td>
<td>• Bottom up</td>
<td></td>
<td>• Potential blow-ups do not wait 6 months</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Who owns operations</td>
<td>• Define tolerance limit</td>
<td>• Cross-map &amp; plug gaps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Who owns operational risk</td>
<td>• Outcomes first, causes second</td>
<td>• Test bottom up against tolerance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Internal audit check / assurance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Crisis Management**

- Horizon scan new causes
- Get likelihood down
- Trade-offs

**Every Board meeting**

- Potential blow-ups do not wait 6 months

**Top down**

- Cross-map & plug gaps
- Test bottom up against tolerance
- Internal audit check / assurance

**Define tolerance limit**

- Outcomes first, causes second

**Questionnaire**

- Review strategy/ Business Plan
- Define tolerance limit
- Outcomes first, causes second
1. How do you define key risks?

2. What are your key risks (including major project risks)?

3. How are they measured/quantified?

4. Who is in overall control?

5. Is there a separate risk committee?

6. What is the format of Board reporting?

7. What is the role of NEBM?

8. Do you define and measure risks by reference to inputs, outputs or outcomes?

9. Do you know if there is a statement of risk appetite? If yes, what is it?

10. How do you manage risks?

11. What’s your capability on:
   - Risk assessment
   - Risk management?

12. Do you link risk performance to appraisals? If so, how?

13. Do you link with other Government Departments on cross-cutting risks? If so, how?

14. How do you take decisions/choose between options?

15. What would be 'failure' of the Department? How does the Board measure success?
## Risk appetite v risk tolerance

### Think about...

<table>
<thead>
<tr>
<th>The words</th>
<th>Betting at the races</th>
</tr>
</thead>
<tbody>
<tr>
<td>'We can only tolerate up to.....'</td>
<td>Risk tolerance sets an absolute limit on how much can be lost on the day</td>
</tr>
<tr>
<td>'We do not tolerate failure'</td>
<td>Risk appetite wants bets to be made where the odds meet a 'good enough' target. But override by a tolerance limit</td>
</tr>
<tr>
<td>'We have an appetite to do.....'</td>
<td></td>
</tr>
</tbody>
</table>

Tolerance is about strategic plans and ensuring delivery; Appetite is about doing things and maximising within limits (i.e. taking certain risks)

Risk appetite is a more complex concept well suited to private sector entities; quite difficult to use in public sector where 'failure' is less obvious
Outcomes v causes

- Success/Failure outcomes are less obvious in public sector
- Typically balanced score-card → several strategic outcomes to consider

- Tolerance → Outcomes → Causes → Actions
  (including combinations) (Mitigations)

- Links with delivery of strategy & managing strategic risk

Example

Outcome = Party X losses German Federal election on Sunday
Possible Causes = Leader’s personality
Economy
Recent history/experience
Policy messages
Etc

Can they compound?
Alignment

- Traditional operational risk register by cause reports to Leadership Team

- Leadership Team Challenges on each cause 'could a big enough blow-up from this cause result in the organisation going beyond tolerance?' Any items with a 'Yes' go on to the Board’s meeting report

- Board independently asks each meeting 'Is anything missing from the list of possible causes?' Any new items go back into the Leadership Team’s register

- End Result. Bottom-up and Top-down with full alignment. As required by Managing Public Money
## Reporting

<table>
<thead>
<tr>
<th>STRATEGIC PLAN</th>
<th>Outcome</th>
<th>2013/14 Metrics</th>
<th>Likelihood</th>
<th>Trend since last Board</th>
<th>Actions allowed for in likelihood</th>
<th>Potential causes</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>T</td>
<td>B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Deliver Aim 1</td>
<td></td>
<td>Red</td>
<td>Green</td>
<td>↑</td>
<td>Main-stream</td>
<td>Black swan</td>
</tr>
<tr>
<td></td>
<td>Deliver Aim 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Deliver Aim 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Deliver Aim 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Deliver Aim 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delivery strategy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Public confidence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Finances</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### T likelihood

- >10%
- 3%-10%
- <3%

### B likelihood

- >50%
- 25%-50%
- <25%
Benefits

- Helps CEO/Perm Sec/Board prioritise what really matters
- Complies with Managing Public Money
- Better risk management of what matters at minimal cost
- Maximises value of input from non-executives (and keeps them out of Executive responsibility)
- Frees up ability to take ‘little’ risks in delivery
- Better decision-making
- Avoids big external consultancy fees
- Addresses all 5 Issues
Attitude to risk of Chief Risk Officers - Gender

Source IRM Culture Survey 2012