apm Specific Interest Group

# APM Risk SiG Conference 26th October 2006
# Reporting risks to the board

## *Purpose*

The purpose of this paper is to summarise the key points from the various presentations and knowledge sharing session held at the October meeting of the Risk SiG. It should provide a reminder for those at the event of the main issues, tips and suggestions for reporting risks to the board. It may also be useful for anyone not present who has an interest in this topic.

This paper should be read in conjunction with the presentations which are available for viewing at http://www.apm.org.uk/riskmanagement/page.asp?categoryID=11&subCategoryID=&pageID=&action=viewArticle&category=75&uID=&ID=525

## *Scope*

The target audience for this paper is predominately project and programme managers. However others involved in operational or business risk would find many of the ideas useful.

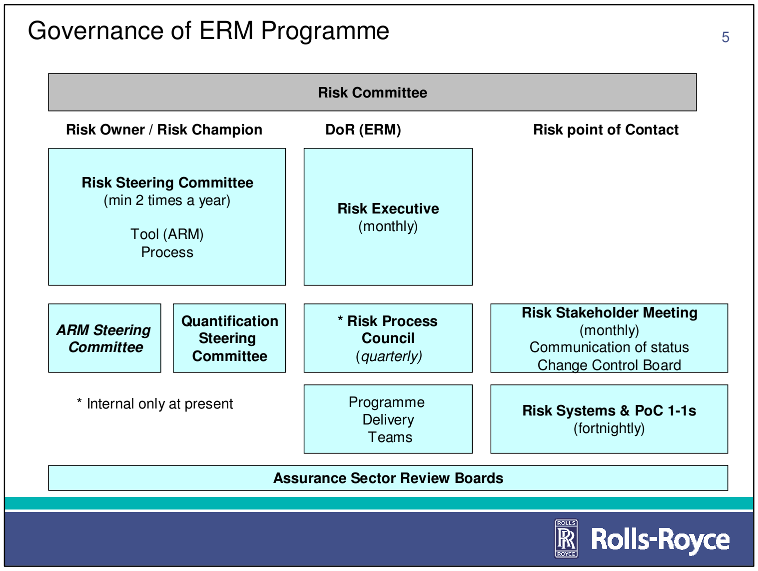
## *Introduction*

The presenters were asked to provide their views on reporting risks to the board. They were given a brief which highlighted 4 topics for consideration and were asked to reflect on those areas from as many perspectives as possible. After the main presentations the delegates split into 4 Knowledge Sharing Network (KSN) groups to discuss each topic. Whilst the body of this paper maintains that structure, many of the key points were identified several times in different areas. For simplicity each key point has been placed in its predominant section.

## *Governance*

There were 5 key points identified in this topic:

- ***Bodies***
  It is necessary to have a clear understanding of which parts of the organisation are involved in the risk process. Both BT and Rolls Royce have a clear framework diagram that explained the groups involved and also how information flowed between them.




- ***Stakeholders***
  Stakeholders – a common theme is to ensure that stakeholders are identified and engaged as they offer a different perspective and a broader range of possible impacts.
  Some stakeholders will identify strategic risks which may need to be managed at the Project Sponsor level. Any effective risk process should provide an identification of the widest range of risks and should have a contribution from stakeholders.

- ***Appetite***
  One important prerequisite for helping to determine the level of detail required for risk reporting is to know the Board's risk appetite. As Protiviti explained "establish the big rules including appetite and ask are the risks undertaken consistent with the organisation's risk appetite?

- ***Culture***
  The term culture towards risk management is used a lot but without much detailed definition. For many it is the attitude to risk combined with the risk appetite that generates a culture. Clearly every individual on a board will have a different attitude to risk but collectively the board will promote a particular risk culture – either consciously or subconsciously, tuning in to that culture is very important, especially if you want to try and change it.

- ***Common Language***
  When reporting risks to the board you must ensure that the terminology used will be clearly understood by the recipients. This implies that a common risk language be used across the business and this can be defined as part of the risk policy or the risk standards.

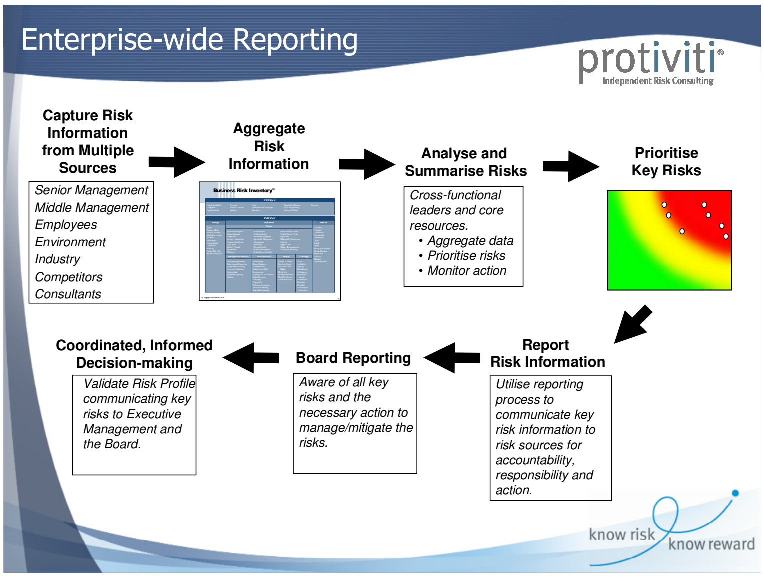
There were two additional points raised during the governance KSN.

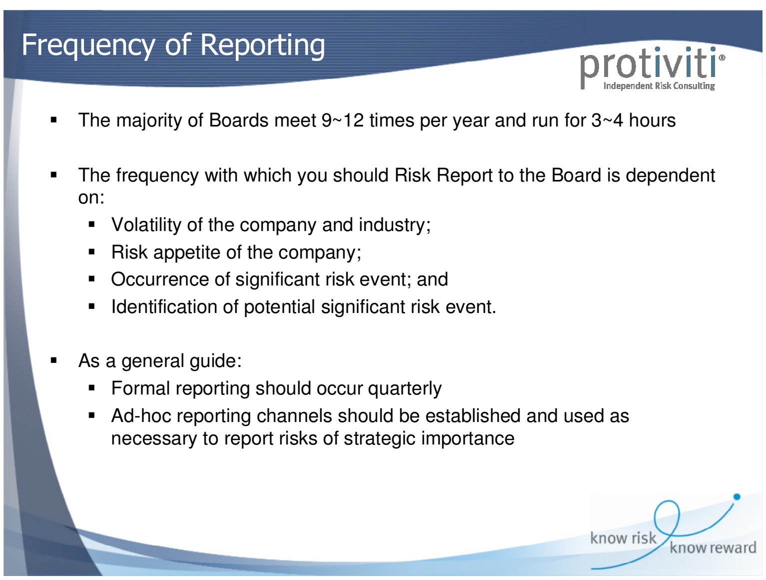
- The first was how to convince the Board that they own governance of risks. A comment was made that it is active ownership that is needed. One suggestion for supporting the board was to offer a "Masterclass" in risk management. It was also recommended that the board members be approached individually.
- Some boards may not fully understand project and risk management – but can't admit it. One suggestion for this is to get them to actively manage a single risk with support.

## *Receiving information*

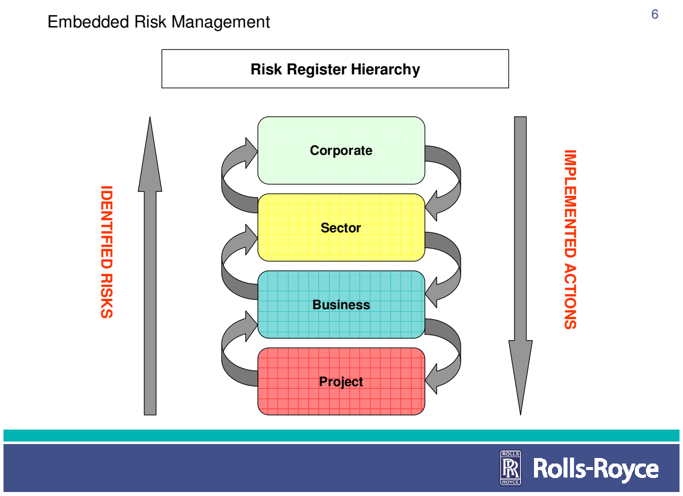
There were 3 key points identified in this topic.
This topic was slightly modified during the analysis to include any process related suggestions.

- ***Process – frequency***
  Everyone agreed that there should be a defined risk process, however the frequency of reporting to the board was dependent on the industry and the organisation but should be at least every 6 months with some form of escalation in place for any new emerging or rapidly changing risks.
  Protiviti explained this clearly in their presentation:



- *Top down and bottom up*
  Must undertake bottom-up analysis and flow of risks as well as top-down. This was mentioned by most presenters and is succinctly demonstrated by this slide




The bottom-up is, of course, to capture those big or common risks. The top-down is to ensure that the lower levels understand the risks which the higher levels are managing allowing them to help and see that their big risks haven't been discounted. HVR explained "Strategic risks help structure risk identification at the lower level. You should be able to relate tactical risks to strategic risks.

- *Concise top level with supporting documentation*
  It is important to ensure that an appropriate amount of information is presented at all levels and that means at the top-level you need to report the information in a simple, concise way.

## *Reporting of Risk*

The 5 key points were:-

- Understand what the Board require to help them make decisions

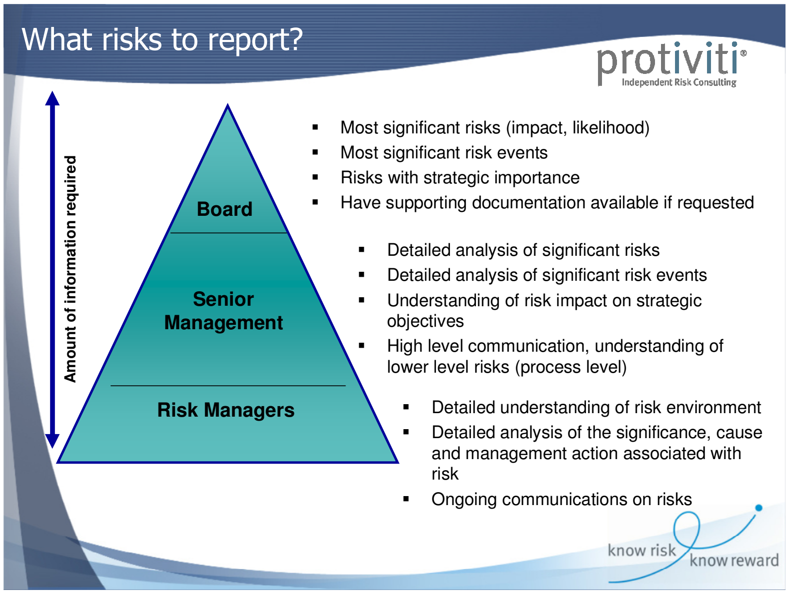
  What does the board want? – Find out! The board may not know what they want. Use what we have got and try to anticipate what they want.

- Aligned with strategy and objectives.

  What is the board strategy? Is it finance, or sales, or expansion, or customer satisfaction based? Risk must impact on corporate strategy/objectives. Rolls Royce explained the risks need to be presented in financial terms and in how they impact on the strategic objectives. Thus Rolls Royce can target mitigation resources at key risks. BT explained "Enterprise threats are discussed at Board level and appear in the Annual Report. An example of a strategic risk is the pension fund is large compared with the size of the company."

- Effective communication/ presentation sympathetic to the organisation's culture.
- Present the few key (5/6) risks across the organisation.
- Right Information at the right time

  Protiviti summed this up by:

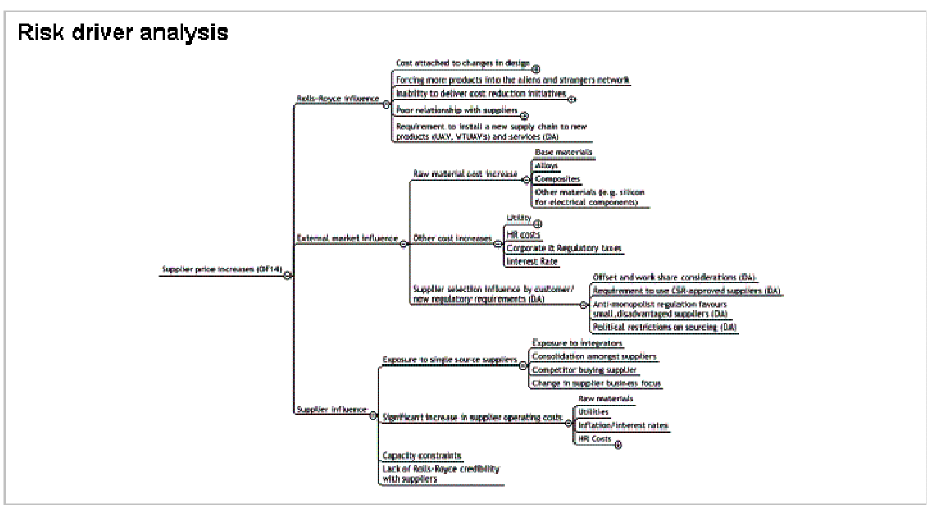



## *Tools and Techniques*

One technique identified or referenced by most presenters was:

- Cause and effect – sensitivity graph (driver analysis)

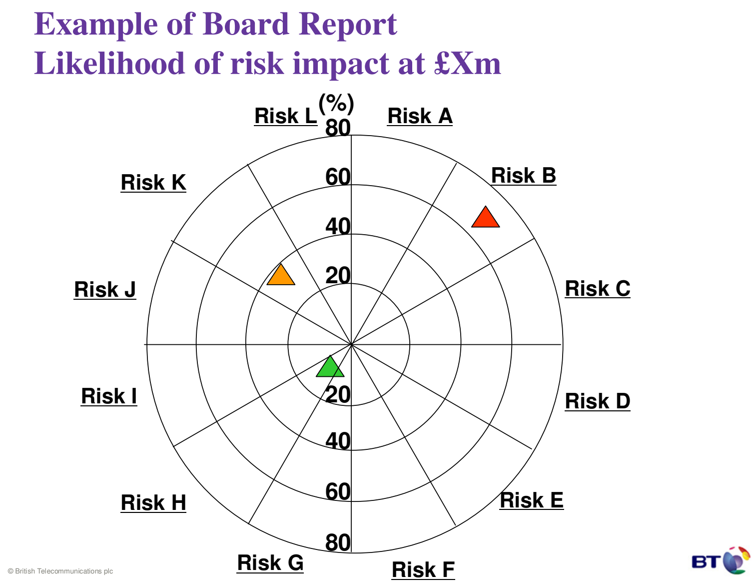
  This aspect came out in different ways in the presentations but they were saying overall that it is important to consider how the risks' causes and effects are linked so that a model (e.g. quantitative) can be produced or resources can be addressed at the key risk drivers in order to maximise return on effort managing risks. One aspect of this can be demonstrated by the below from one of Rolls Royce's slides:




The large group of about 20 people in the KSN agreed that there were two additional key points:

- Need a suite of tools which can operate at all levels (but these would depend on the maturity of the organisation)

  BT explained that they use a collection of tools including one to produce their risk dashboard:-




Rolls Royce are implementing an enterprise-wide tool (ARM). Many organisations use cheap tools, e.g. Excel, and can't justify the expense of a heavyweight tool but still want the benefits of hierarchical risk management. The feeling was that this could be achieved.

- Need some consultancy to help the organisation to implement this,

  This was so that the company can have a common language, education, expertise in the tools & techniques available and someone to drive the implementation. This could well be from within the company. Strategic Thought said "Use a common terminology, categories that reflect the organisation."

## *Conclusion*

Overall the conclusion is to ensure that the boards expectations of risk management are understood and that the reporting of risks is done in a way that provides valuable information at the right time to enable the boards to reduce surprises, to link operational risks with strategic decisions and recognise when their risk exposure or their risk appetite changes. It should be simple and clear although the supporting documentation should be available if needed.

## *Acknowledgements*

Thanks very much to all of the presenters who have made their material available.
Larry Stone, BT
Tom Teixeira, Rolls Royce
Martin Hopkinson, HVR
Karl Davey, Strategic Thought
Jonathan Blackhurst, Protiviti