

**Deloitte.**

# Practical Management of Material Business Risks.

*Insights into an enhanced risk management program*

Craig Mitchell  
Partner, Risk Services  
2008

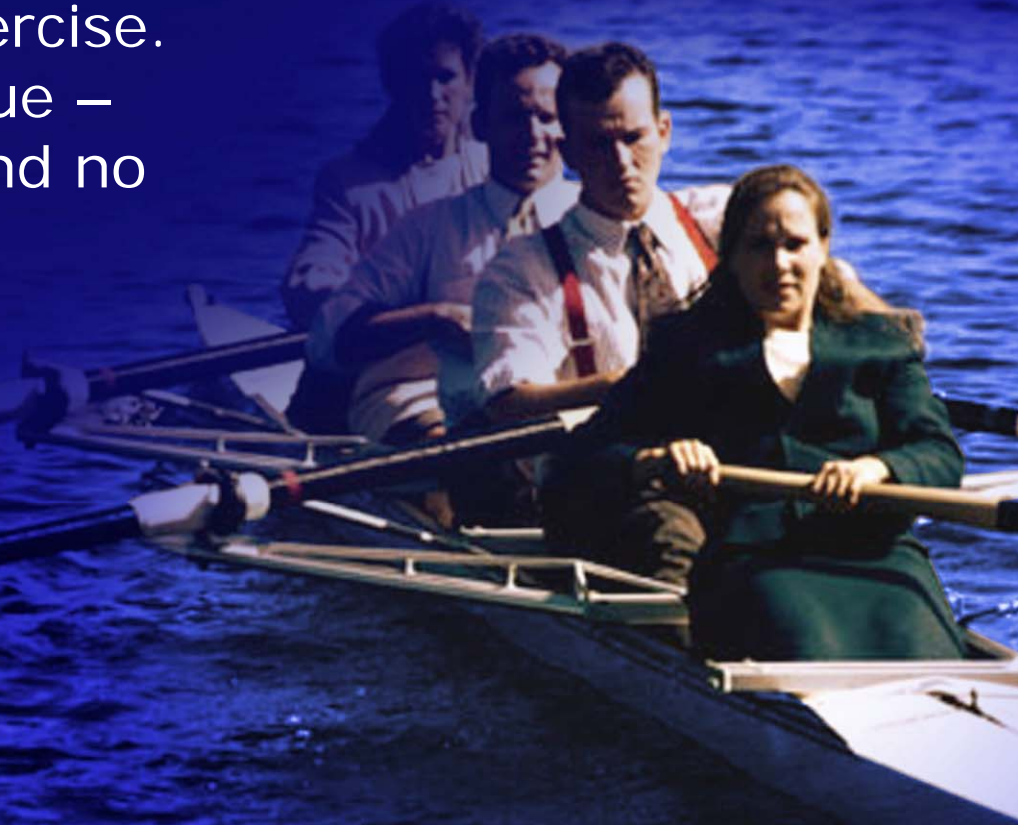
**Raise your risk IQ.**



Risk management is a journey.

It is about an organisation's culture, processes and structure.

It is not a tick-the-box exercise. Every organisation is unique – there is no right answer and no wrong answer.



# Agenda

- Warning signs to enhance your risk management program
- Risk approach insights:
  - An effective risk management system
  - Identification
  - Rating/definition of material business risks
  - Effective management
  - Reporting
  - Efficiency
- Outcomes/benefits
- Closing remarks

# Warning signs to enhance your risk management program



# Warning signs to enhance your risk management program

- Organisational change
- Changing external environment
- Corporate growth
- Pockets of strong risk management but lacks uniformity and consistency
- Limited awareness of risk management
- Limited consensus/discussion on risks
- Focus on risk identification, but then what?
- Poor risk reporting, if any
- Credit rating agencies
- True compliance with Principle 7

*“Just need to formalise it and take it to the next level”*

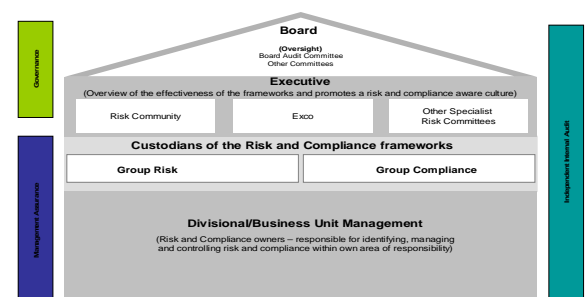
# Risk approach insights



# Risk approach insights

## - An effective risk management system

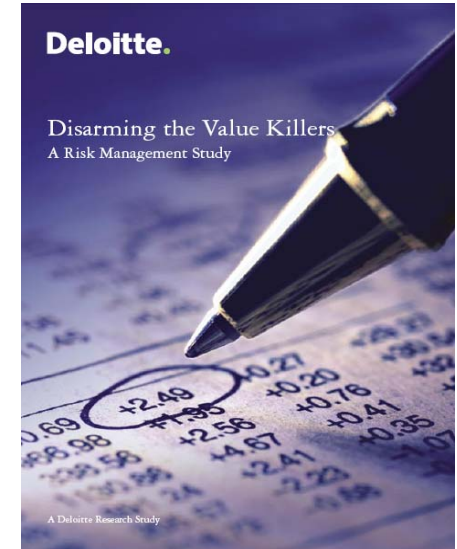
- Should have regard to:
  - the company's objectives
  - the company's internal organisation
  - the environment in which it operates
  - the degree of risk willing to be accepted (the company's risk appetite)
  - the company's culture
  - cost-benefit issues
- Management risk community group
- Describe and tie governance elements together pictorially
- Is dynamic and should be regularly evaluated/benchmarked
- Regular corporate profiling to reinforce and keep it fresh
- Getting this right will ensure a fit-for-purpose system for your company



# Risk approach insights

## - Identification

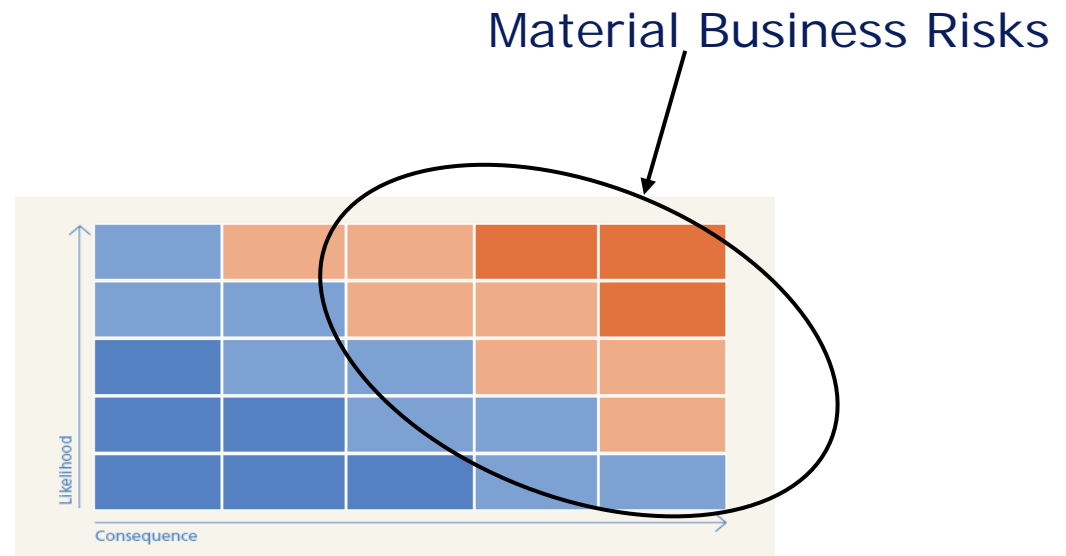
- Align and link with corporate strategy/plan process
- Corporate-wide and all risks
- Inherent risk focus
- Consider both top-down and bottom-up development
- Use facilitated workshops – ensure consensus and feedback changes
- Sanity check with environmental scans
  - Deloitte's *Disarming the Value Killers*:
    - o Critical risk interdependencies
    - o Strong ethics and control culture
    - o Low-frequency high-impact risks
    - o Timely information



# Risk approach insights

## - Rating/Definition of material business risks

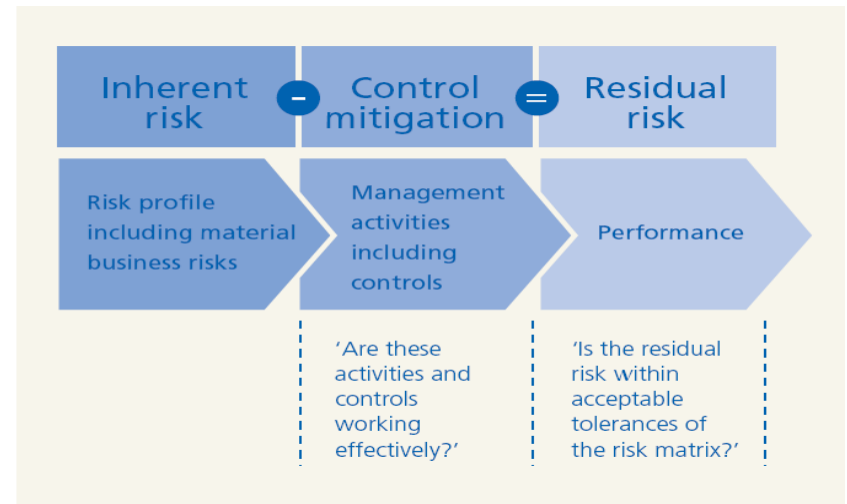
- Development of “material business risks”
- Pictorially displayed through consequence and likelihood risk matrix:
  - Fully defined quantitative and qualitative consequence definitions:
    - o covering criteria important to the company such as financial, OH&S, etc



# Risk approach insights

## - Effective management

- Not about eliminating risk but whether the residual risk is within acceptable tolerances of the risk matrix
- Some risks cannot be managed & some may not be cost-effective to manage
- So focus should be on:
  - Effectiveness of control mitigation -> COSO internal controls + internal audit
  - Residual risk - understanding, awareness, response
- Business owns the risk
- Align accountabilities for risks
- Be clear on the risk response:
  - Actions?
  - Reporting?
  - Assurance?
  - Oversight?



# Risk approach insights

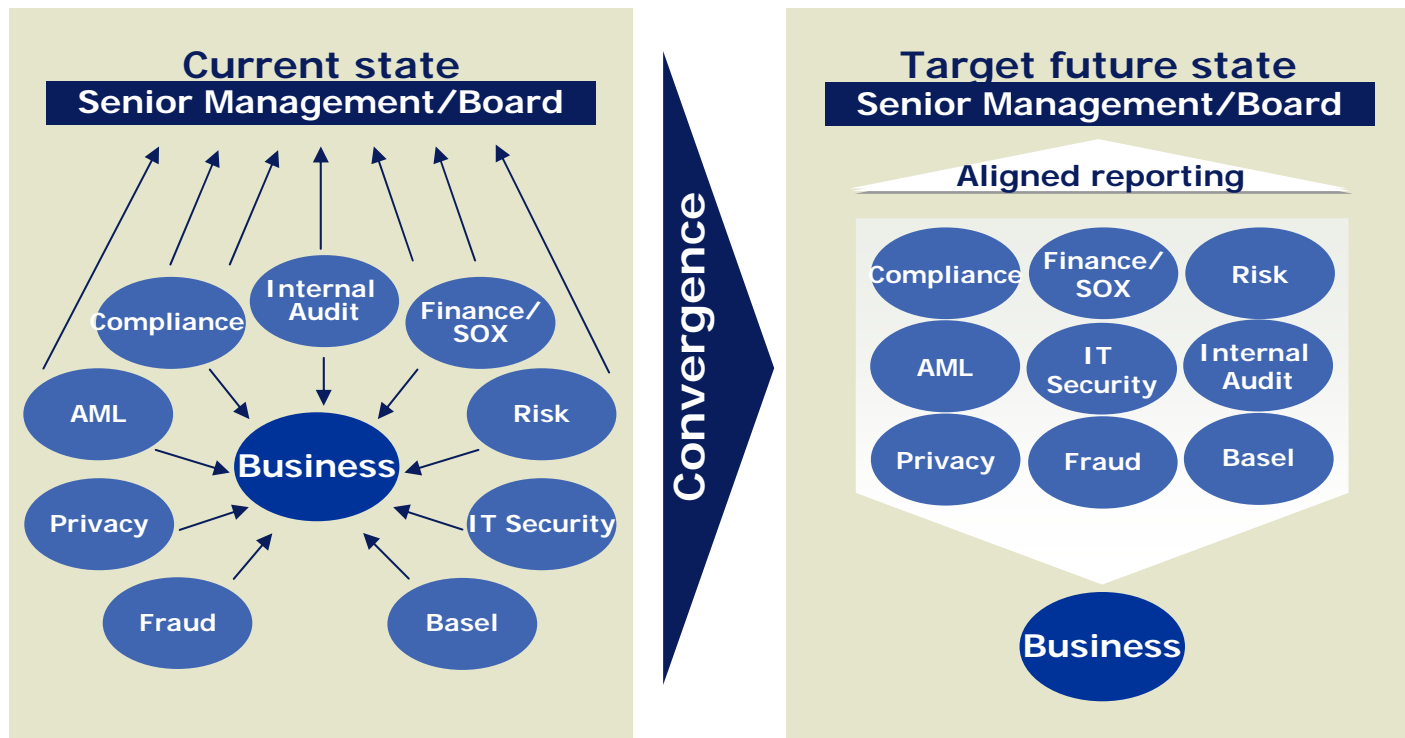
## - Reporting

- 7.2 not about “sign-off” but “reporting”
- Possible elements:
  - Individual risk profile reports:
    - o Throughout year
    - o Detail and frequency consistent with risk rating
    - o Content can include – description, rating, direction, context, controls/response, assurance, action plans, history log
    - o Business presents to Board
  - Annual summary report:
    - o Outlines the process throughout the year – policy, system, matrix, identification/rating, individual reports
    - o May contain conclusive statement
  - Internal audit:
    - o If requested by Board

# Risk approach insights

## - Efficiency

- Need to design to not burden the business
- Converge and align with other functions



# Outcomes/benefits



# Outcomes/benefits

- **Fit-for-purpose** risk management system to support your strategies/plans
- Greater transparency/consensus on risks
- Better understanding of risks
- **Enhanced communications** between Board, executive management business
- Clearer risk mitigation and actions with appropriate key risk indicator reporting
- Aligned accountabilities
- Efficiently converged with other functions
- Risk tools and education
- Break through “buzz” words
- Compliance with Principle 7

# Closing remarks



# Closing remarks

- Acknowledge new Principle 7 is different and has raised the bar
- Recognise risk management is about culture and therefore takes time...it is a journey
- Ensure you can tie all risk elements together in a demonstrable way
- Seize the opportunity now with the implementation of this new Principle to raise your company's risk IQ
- [www.deloitte.com/au/corporate\\_governance](http://www.deloitte.com/au/corporate_governance)
- [cmitchell@deloitte.com.au](mailto:cmitchell@deloitte.com.au)

**Deloitte.**



## Recognise and manage risk

A Guide to compliance with ASX Principle 7

August 2008



This document is provided as general information only and does not consider your specific objectives, situation or needs. You should not rely on the information in this document or disclose it or refer to it any document. We accept no duty of care or liability to you or anyone else regarding this document and we are not responsible to you or anyone else for any loss suffered in connection with the use of this document or any of its content.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/au/about](http://www.deloitte.com/au/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms.

Liability limited by a scheme approved under Professional Standards Legislation.

© 2008 Deloitte Touche Tohmatsu. All rights reserved.