



# Our risk profiles...



- ✦ Australia biggest risks... stingers, snakes and English tourists.
- ✦ The US has a proud history of risk managing its interests - Australia has a long history of redefining ours after a change in Government.

# Risk Management Culture



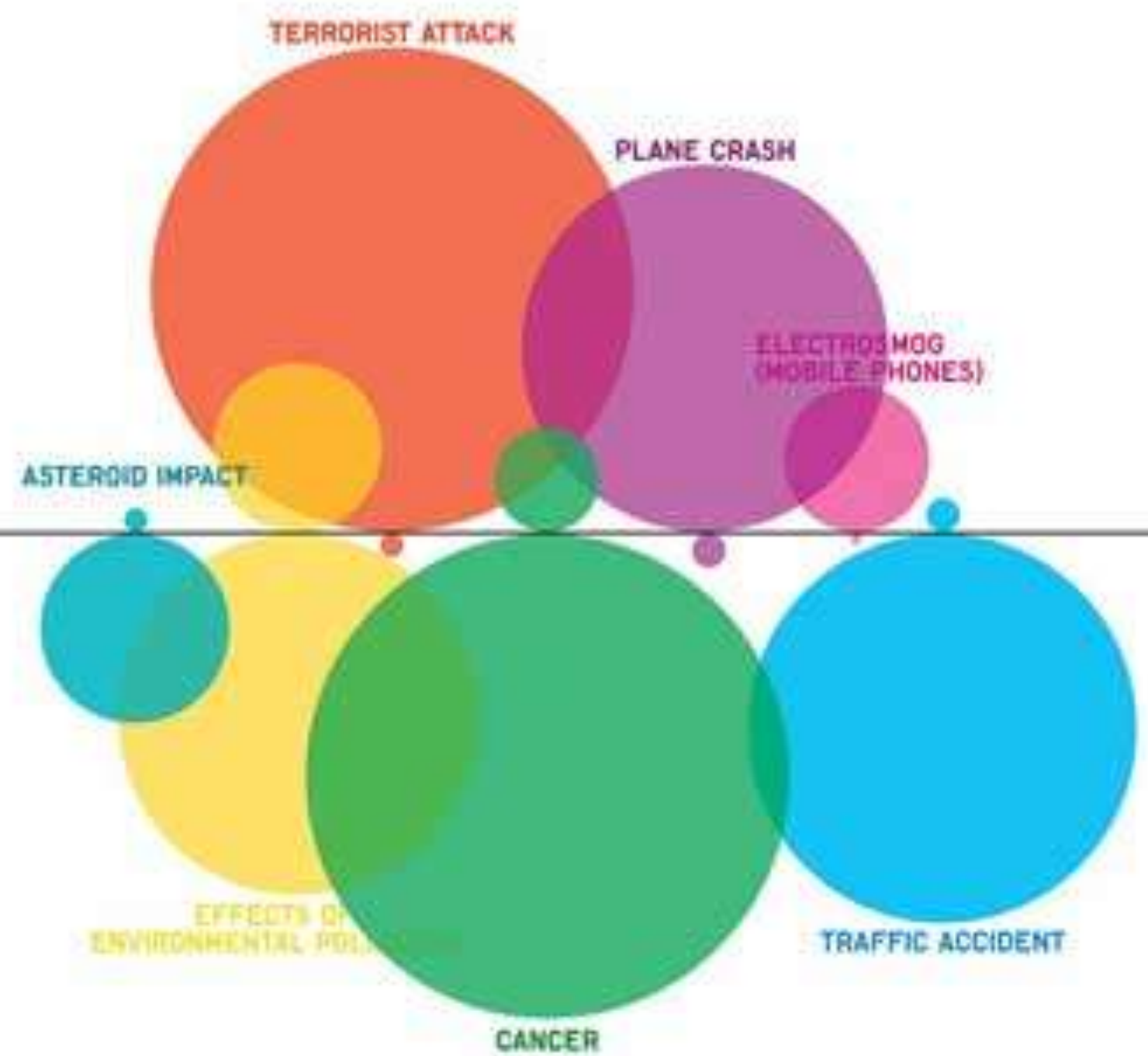
- ✦ She'll be right mate...
- ✦ If at first you don't succeed... get a bigger hammer!!!

# Risk takers or avoiders?

<b>Derivatives trading</b>	<b>Skydiving</b>	<b>Abseiling</b>	<b>Motorcycling</b>
	<b>Multi-day hiking</b>	<b>Pilots license</b>	<b>&gt;5 speeding tickets</b>
<b>(Illegal) drugs</b>	<b>Rock fishing</b>	<b>Scuba diving</b>	<b>Lumberjack or forestry</b>
<b>Firefighter</b>	<b>Oilrig worker</b>		<b>Worked at heights</b>
<b>Rock climbing</b>	<b>Mountain biking</b>	<b>Skiing</b>	<b>Helicopter flight</b>

**PUBLIC OUTRAGE**

**ACTUAL HAZARD**



**CAUTION**

**THIS SIGN HAS  
SHARP EDGES**

**DO NOT TOUCH THE EDGES OF THIS SIGN**



**ALSO, THE BRIDGE IS OUT AHEAD**



# Our Similarities



*“Basically, since 9/11 companies perspective and focus on security rose....but like all bell curves and honeymoon periods they dropped in a very short time; within that period, government agencies closed gaps on policies procedures and standards, but companies were left in the cold and left to feast on the scraps and crumbs of organizations such as Homeland Security and the State Department. Organizations such as ASIS, AS/NZS4360, and an attempt by ISO so far have fallen short in getting acceptance as a ‘standard’ in organizations globally.”*

# Our Similarities

- ✦ Our changing but intertwined fates...
- ✦ Our inability to define 'risk', 'threat', etc...

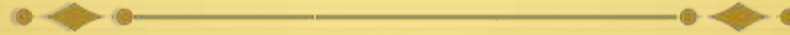


# Our Differences



- ✦ Aussie emphasis on standards and de-emphasis on risk analysis methods
- ✦ US evolution of dozens of risk analysis methodologies, but as yet no security risk analysis/management standards.

# Or to put it another way...



A blunt instrument approach

*Versus...*

Silos of excellence

**Aust.**

AS/NZS4360  
ISO31000

???

Frameworks+++

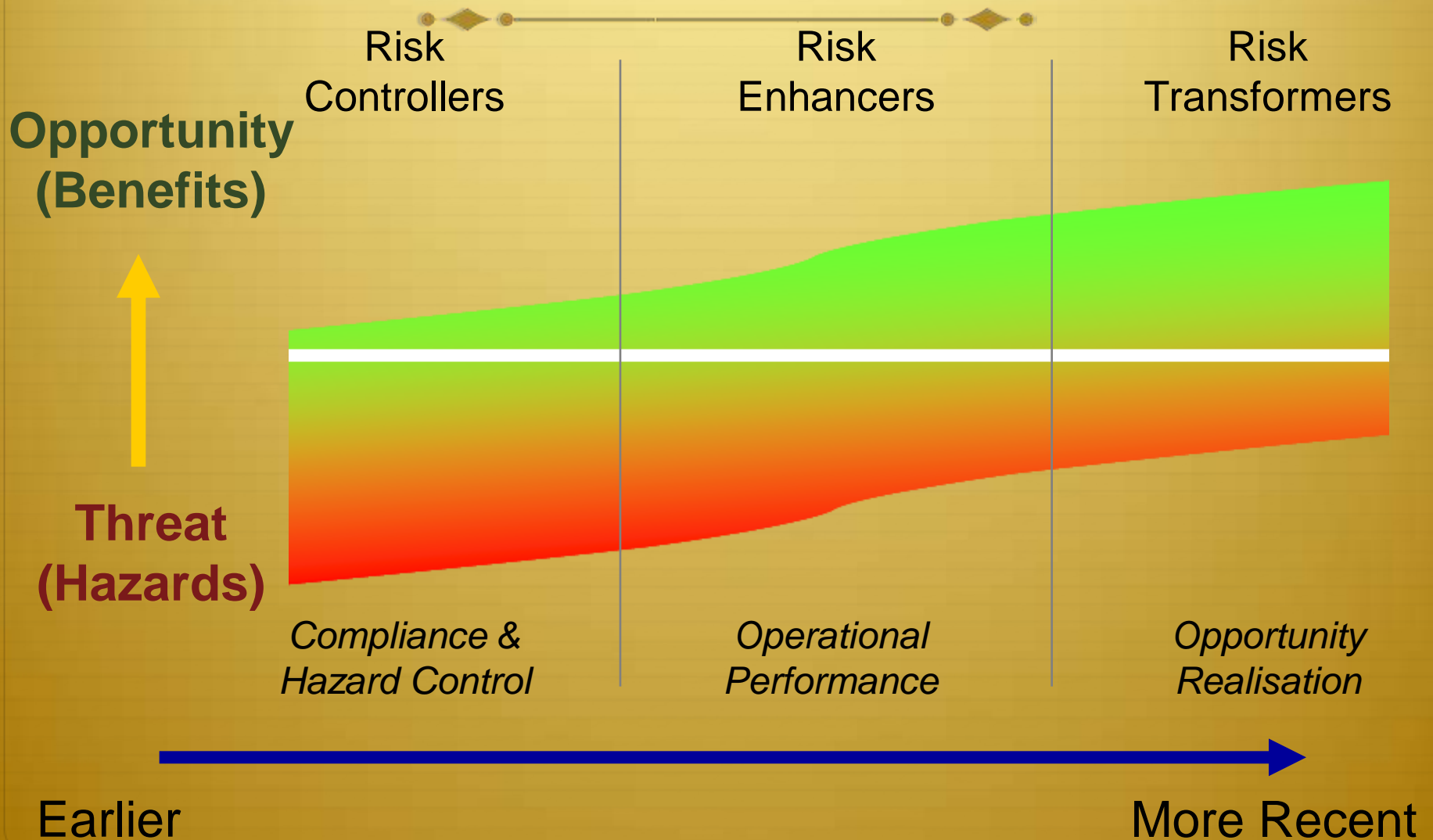
**U.S.**

# Changing Definition of Risk

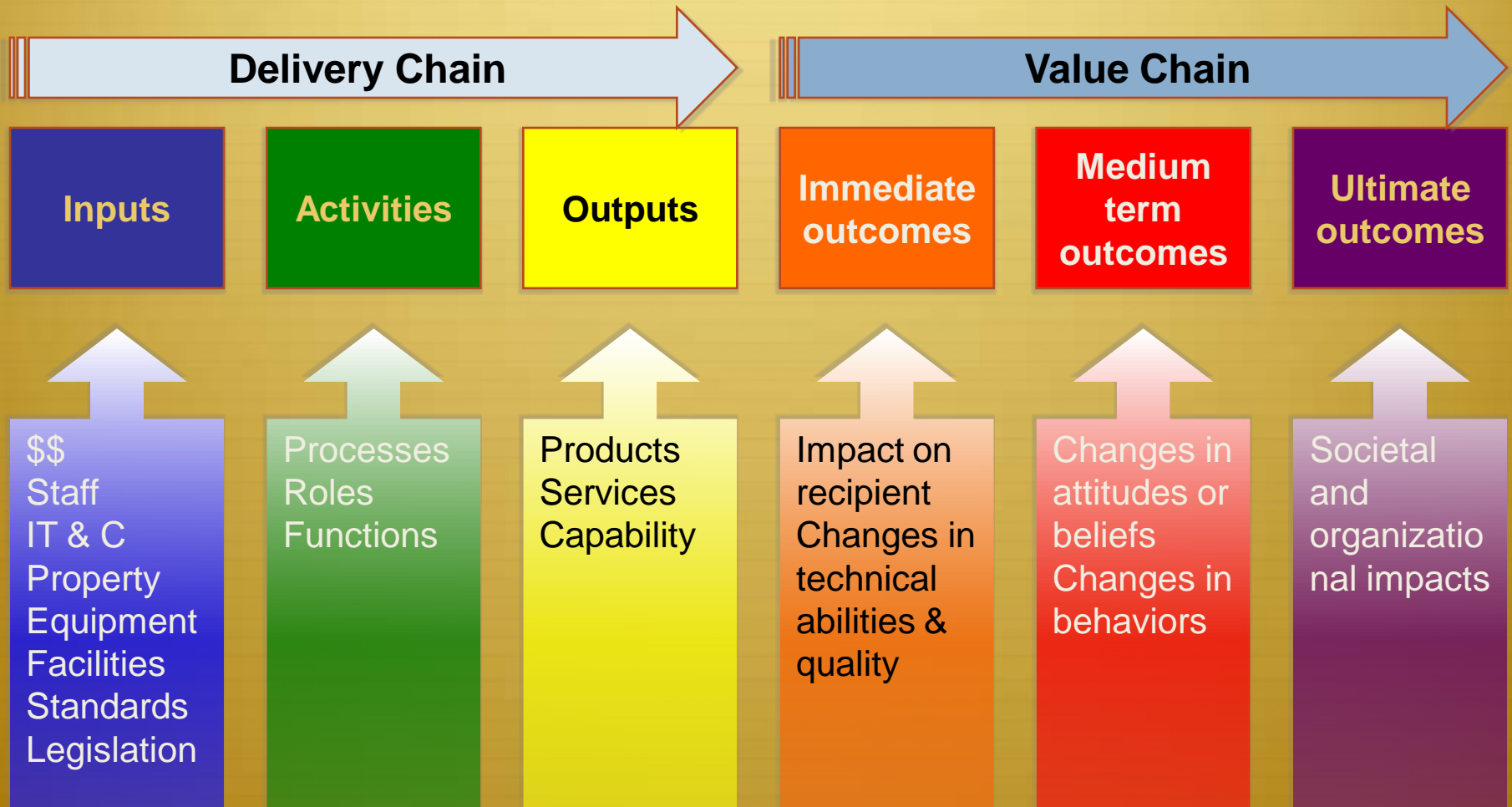


- ✦ *“Measurable uncertainty”*  
Knight, Frank H. (1971), “Risk, Uncertainty and Profit” (University of Chicago Press), Orig. pub. 1921
- ✦ *“Combination of the probability of occurrence of harm and the severity of that harm”*  
ISO/IEC Guide 51:1999
- ✦ *“Combination of the probability of an event and its consequence”*  
ISO/IEC Guide 73:2002
- ✦ *“Chance of something happening that will have an impact on objectives”*  
AS/NZS 4360:2004
- ✦ ***“Effect of uncertainty on objectives”***  
ISO31000: ISO/IEC CD Guide 73 (ISO/TMB WG on Risk Management -2007)

# Hazard and Opportunity



# Value Delivery

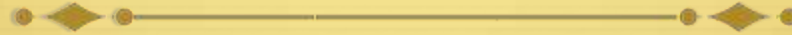


# Changing Risk Management



- ✦ Against the Gods...
- ✦ Probability theory
- ✦ Insurance buying
- ✦ Financial risk (CAPM, Options Theory)
- ✦ Hazard management (Safety, Environment)
- ✦ Embedded risk management
- ✦ Strategic Risk Management...

# Why is it not so simple?



- ✦ Trade offs...
  - ✦ Risk versus perception
  - ✦ Cost versus benefit
  - ✦ Risk versus perspective



# More quotable quotes...

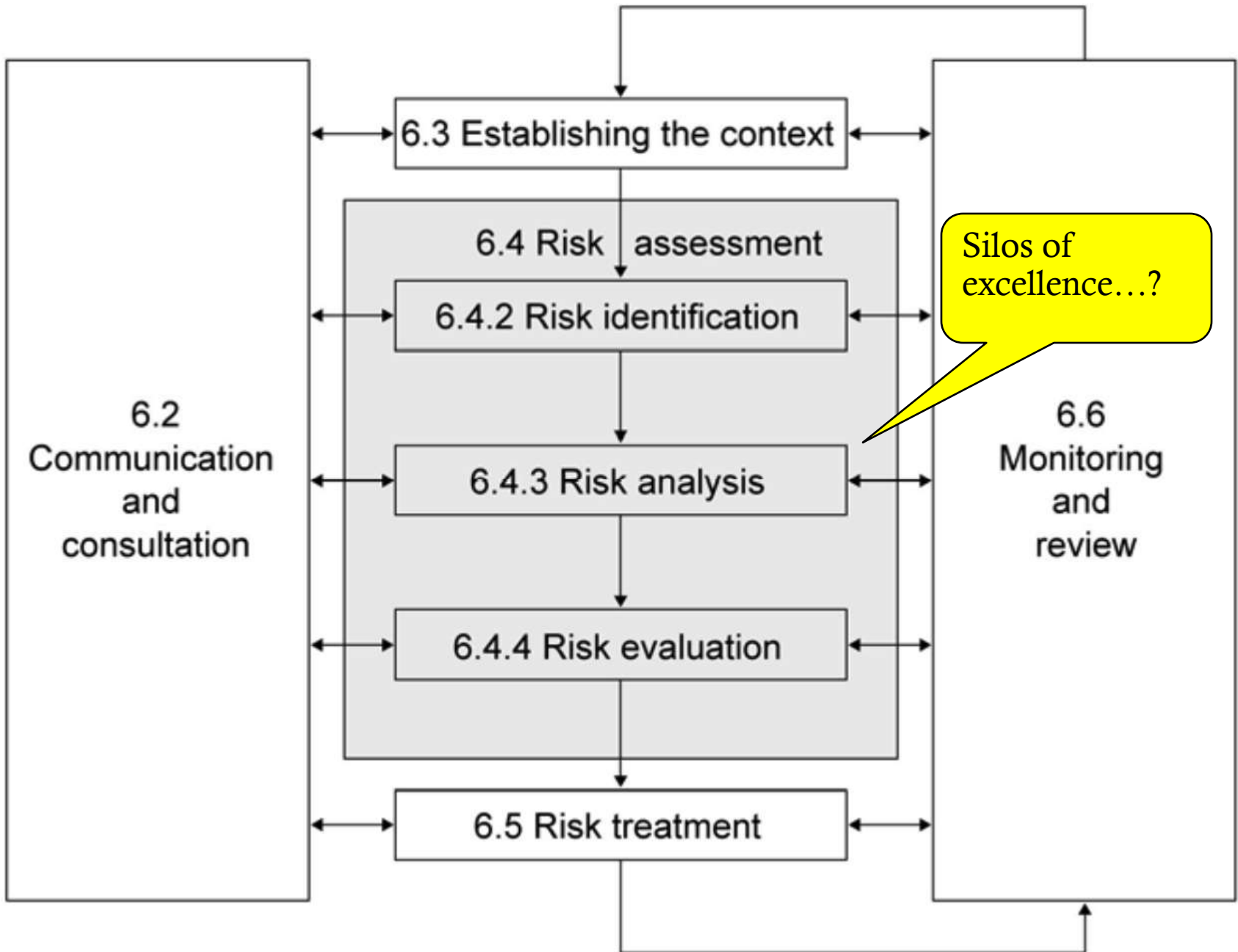


- ✦ *“Americans are more professional than Australians...”*
- ✦ *“My main issue from a corporate perspective being an Australian working for an American Company is that there is no consensus on what should be the standard for security. E.g. IT has standards (SOX), Finance has standards and watchdogs, but security is handled in a total different light to other departments”*

# ISO31000



- ✦ Draft ISO standard is still a flexible guidance
  - ✦ Not prescriptive and not for certification
- ✦ Risk management creates value
- ✦ Not just a compliance exercise
- ✦ Performance indicators are important -What gets measured, gets done
- ✦ Use ISO 31000 principles as 'health check' of maturity of risk management framework and process



Source: ISO31000 Risk Management Standard (Draft:2009)

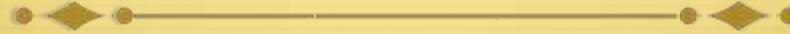


**AS/NZS4360  
ISO31000**

**The Future?**

**Frameworks  
+++**

# Where to now?



- ✦ 'Train smash' or integration...?
- ✦ Alliance or alignment...?
- ✦ Bob...



# Integration



- ✦ Physical, IT, Information, Intel, emergency response, management systems
- ✦ PSCC + EMA = Resilience
- ✦ DESRA → 5 year strategic security plan

# Best of Breed (BoB)...

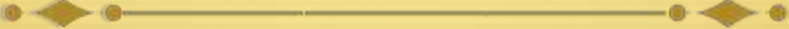


- ✦ Education & Lexicon
- ✦ Body of Knowledge (Eg: SARMA-pedia)
- ✦ Alliances (Eg: ASPTF, CASP, SARMA)
- ✦ Guidebooks (Eg: ISO31000, HB167)
- ✦ Root Cause Analysis & Human Factors

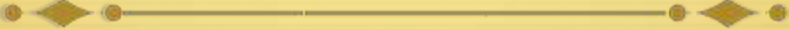
# The Risks.... To SRM



1. Over-regulation
2. Under-regulation
3. Inadequate consultation and cooperation
4. Inaction on our part...



✦ The keystone in our many pillars of resilience, risk management must continue to populate or perish.

- 
- ✦ “Knowing is not enough; we must apply.
  - ✦ Willing is not enough; we must do.”

Goethe

---

# Thank you

Thank you

[Julian.Talbot@jakeman.com.au](mailto:Julian.Talbot@jakeman.com.au)

+ 61 414 341349