

# **What Security Risk Management Means for the Enterprise**

*The Business Case for Proactive SRM*

**Julian Talbot**

Risk Management Institution of Australasia  
Jakeman Business Solutions Pty Ltd

*2nd National Conference on Security Analysis and Risk Management  
George Mason University Law School, Arlington, Virginia*

*15 May 2008*

# SRM - Managing the Unexpected

- # 1 problem for enterprise SRM
- 5 things that you can do about it
- 5 proven strategies for organisational RM
- 8 simple steps to better business cases
- Preoccupation with failure is good!
- Swiss cheese is even better...

**srmbook**



Security Risk Management  
BODY OF KNOWLEDGE



# Our Enterprises...

- Don't take **enough** risk
- Take **too much** risk  
(without realising)
- Over-mitigate risks  
to be **too** low

... are the dominant  
entity of this era



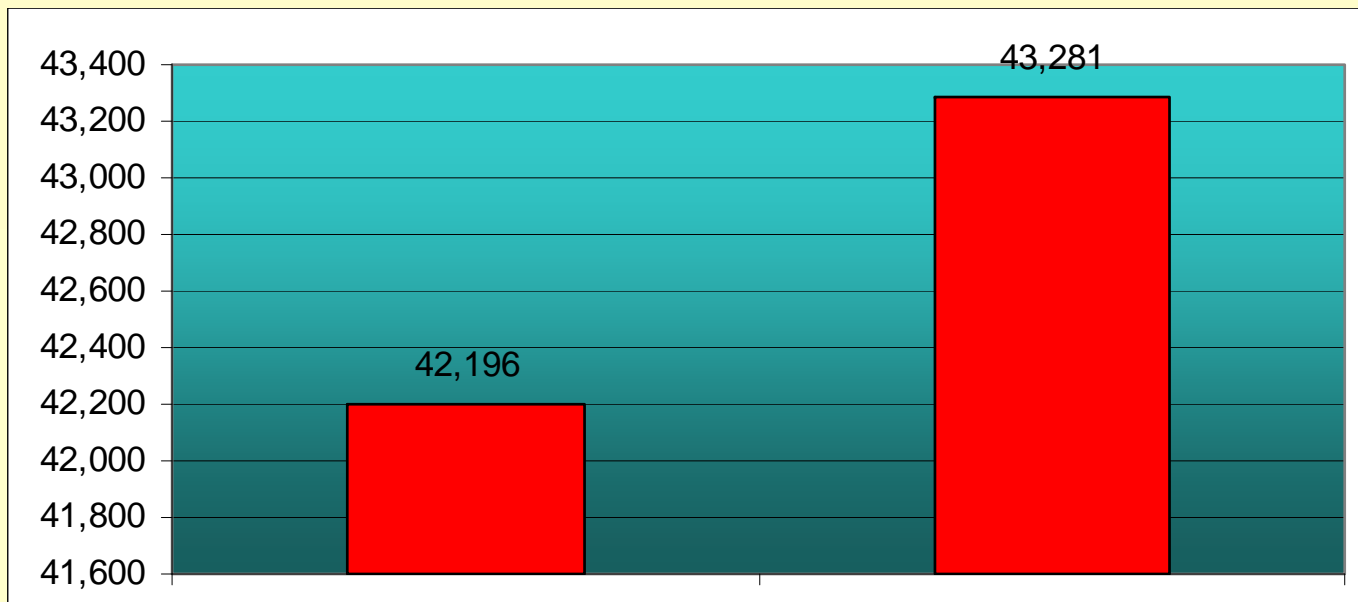
# Risk-Informed Decision Making

- In the US in 2001 there were...
  - 2,974 fatalities in the 9/11 attacks
  - 42,196 motor vehicle fatalities



# Risk-Informed Decision Making

- US air travel in 2002 dropped 30%
- Road deaths increased by 1,085 in 2002
- Despite being previously on a slight downtrend



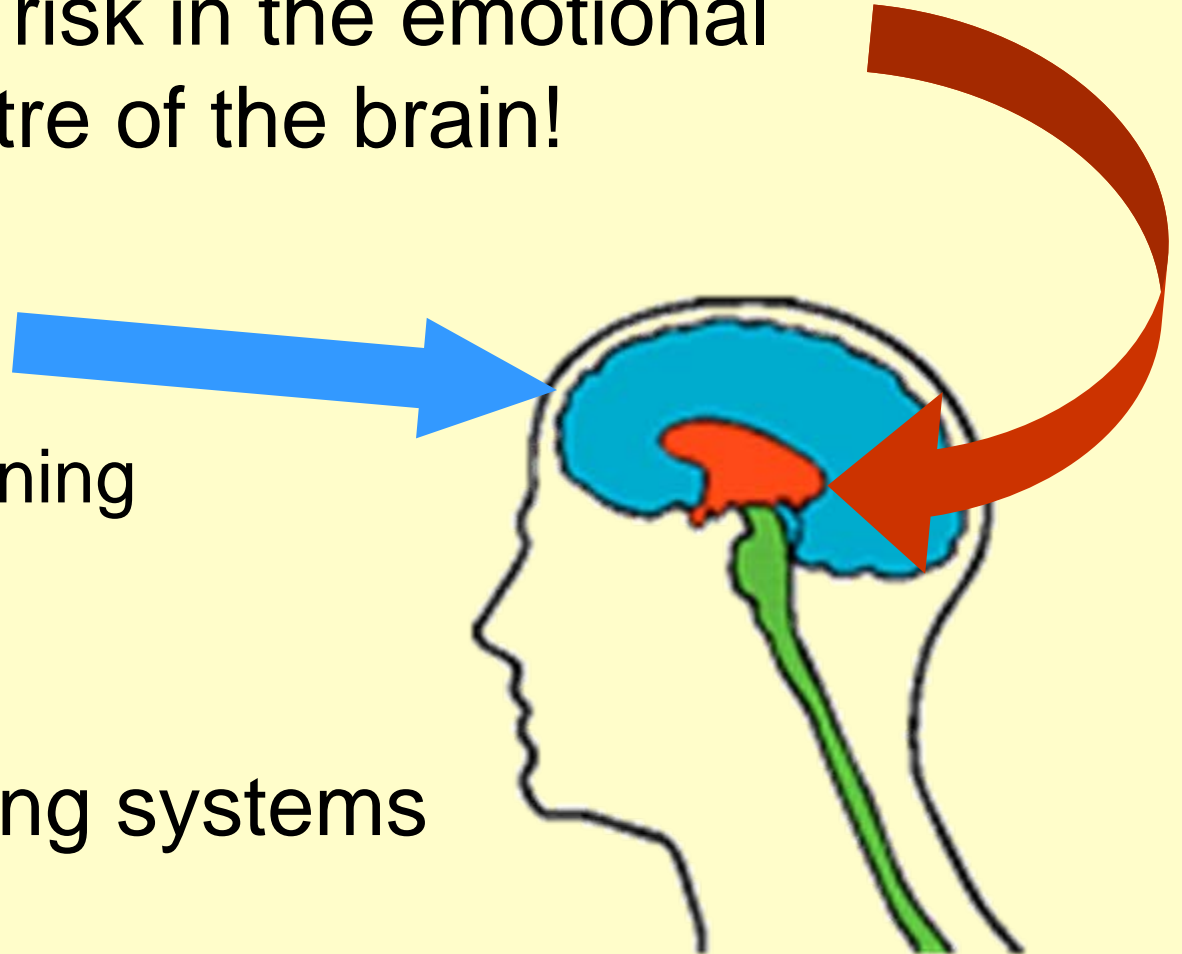
# Who could have predicted...

In December 2001 David Myers wrote:

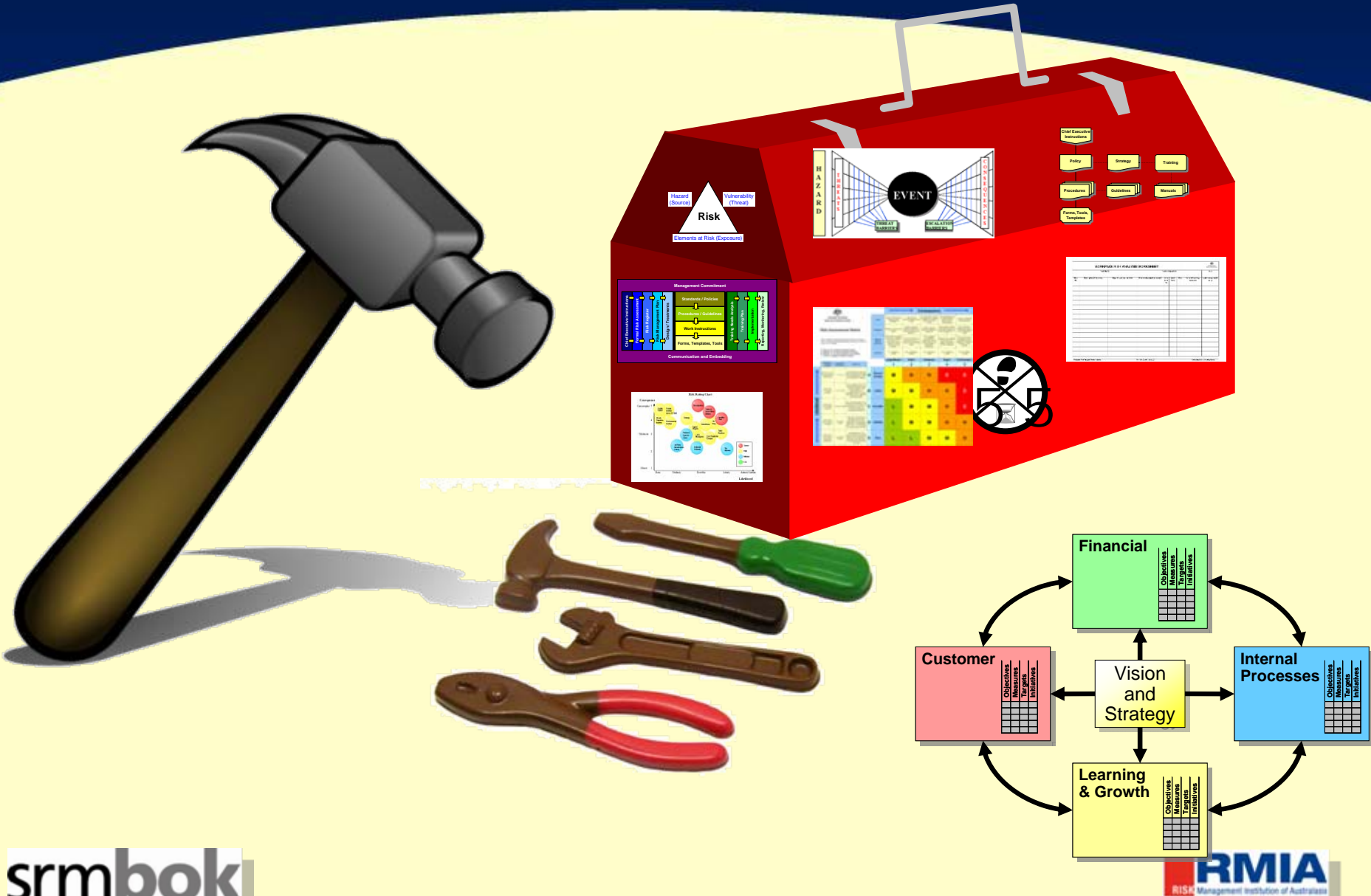
- If Americans fly 20% less and
- Drive half the un-flown miles
- They will spend 2% more time in vehicles
- Resulting in 800 more deaths on the roads
  
- *“Terrorists may kill three times more people on the roads than on those planes...”*

# The number one problem

- We manage risk in the emotional (Limbic) centre of the brain!
- Neocortex
  - logic, reasoning & intellect
- Two conflicting systems



# Things we can do about this...

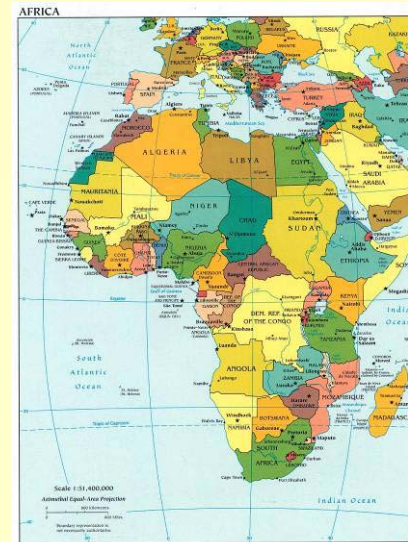


# Things we can do about this...

Use the Limbic system AND the Neocortex:

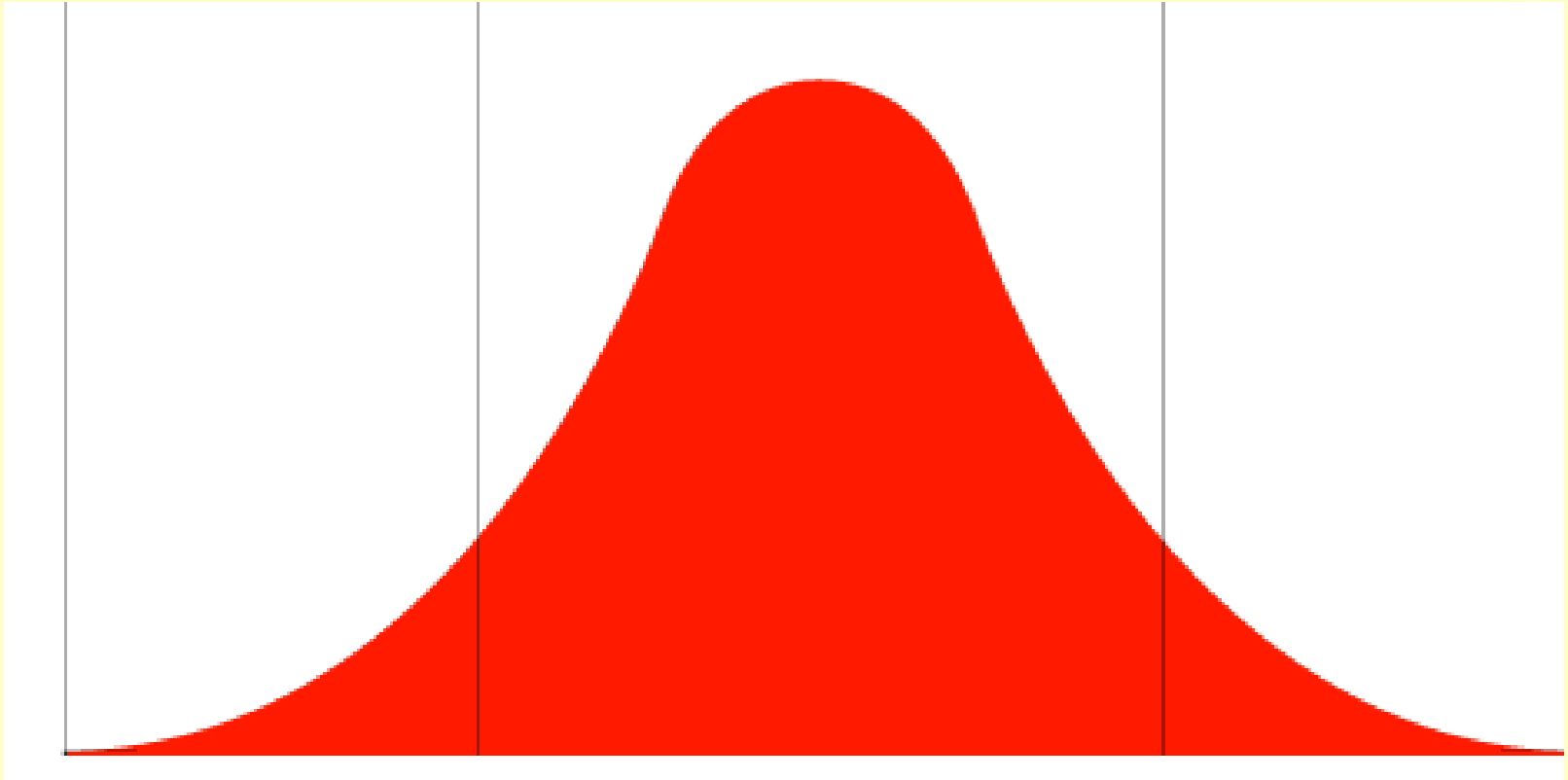
1. Know the business benefits of SRM
2. Assess the maturity levels of the organisations SRM
3. Collaborate, collaborate, collaborate
4. Understand barriers, build Guidelines then Implement!
5. Become better traders...

# The Business Case



# The Threat Environment

No of Organisations



Risk

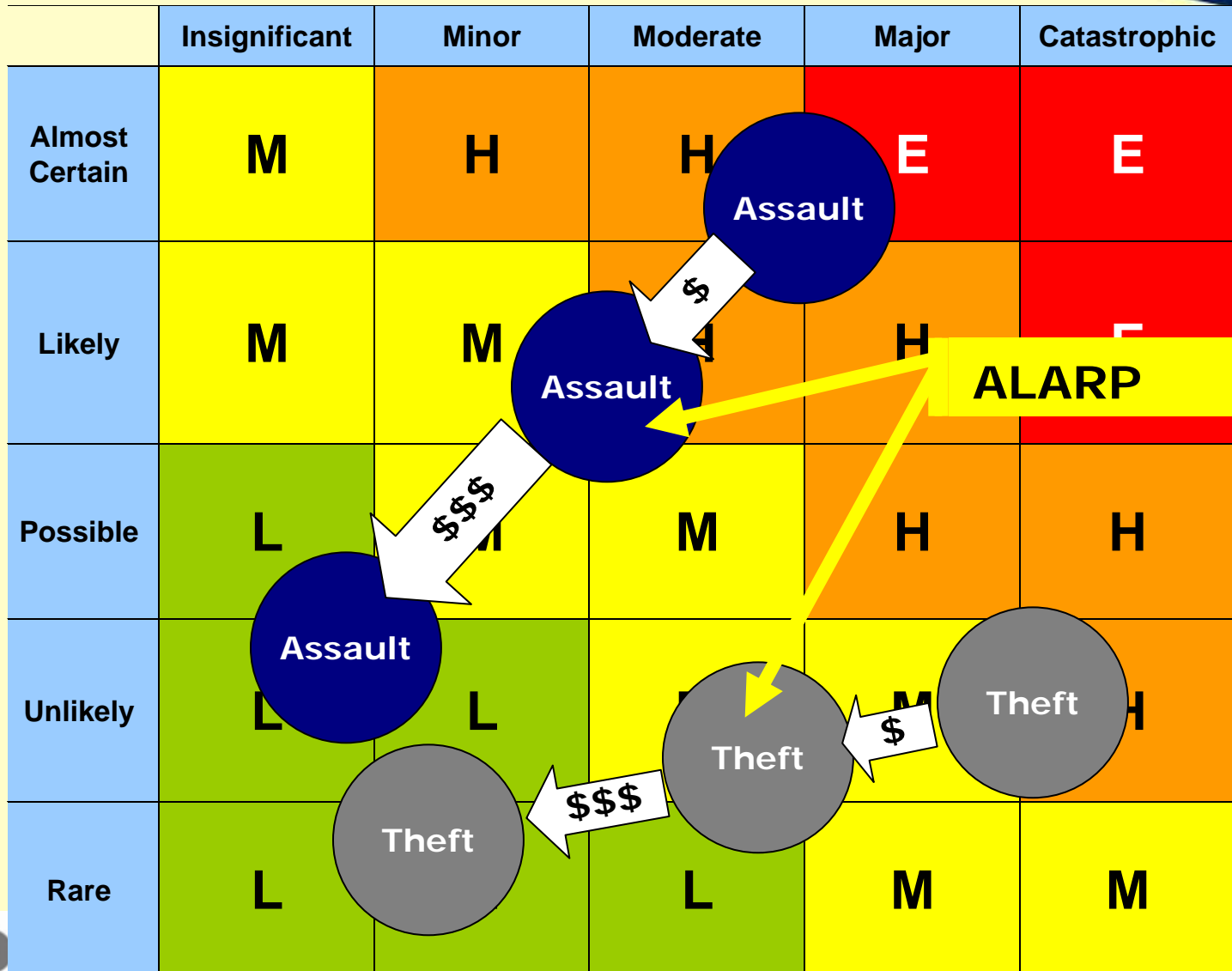


# Business Case for Proactive SRM

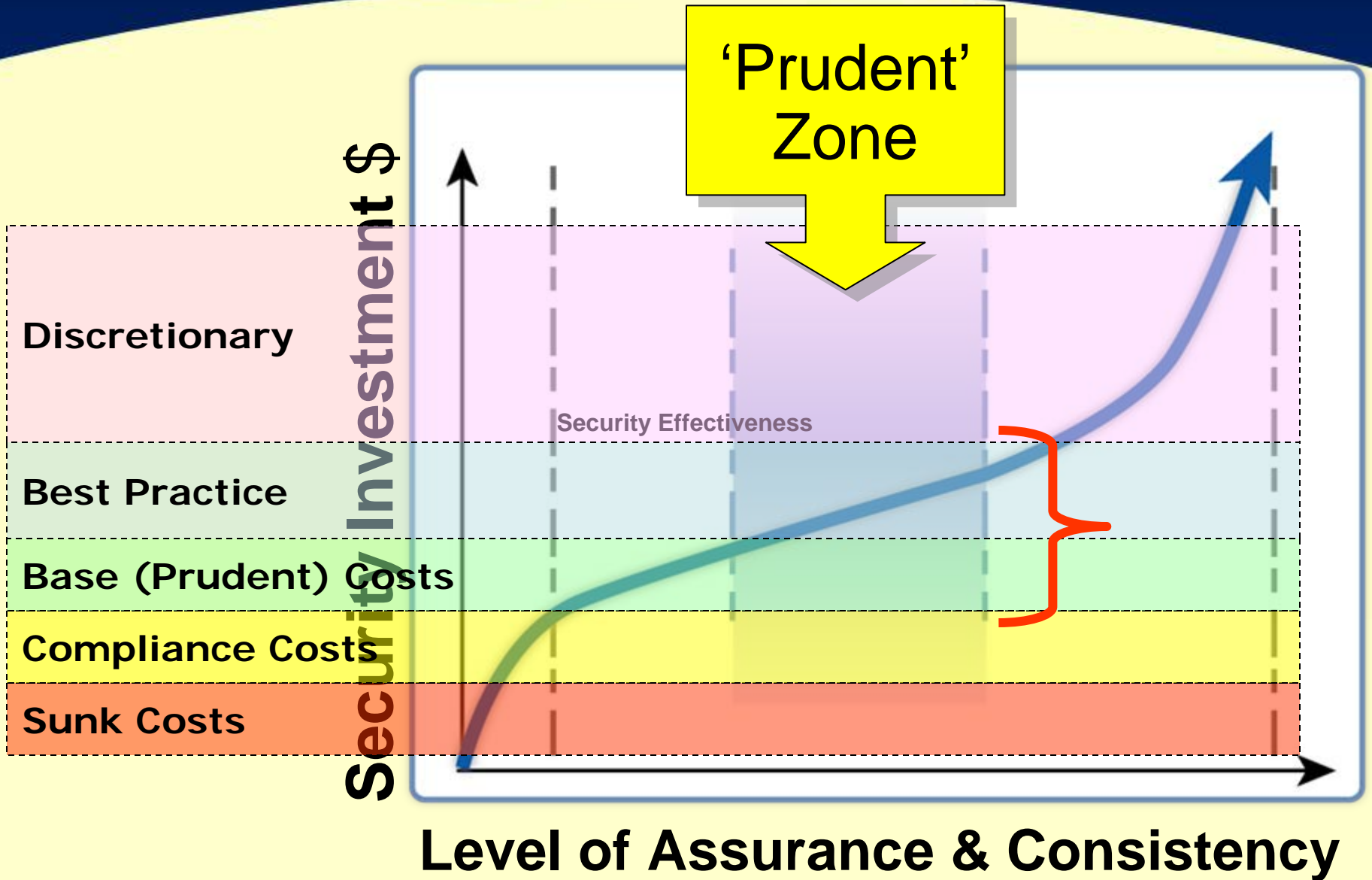
- The Problem...
  - Managers lack structured cost-benefit methods to evaluate and compare alternative security solutions



# As Low As Reasonably Practicable



# Cost Effectiveness

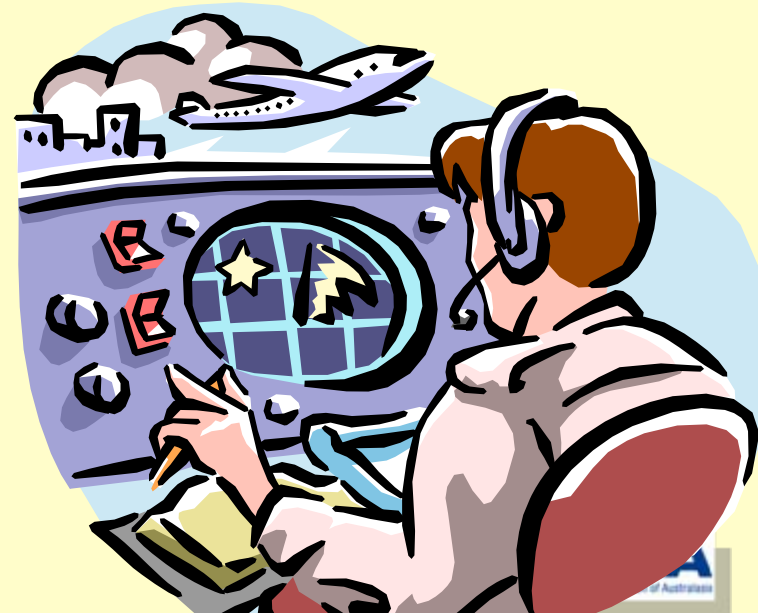


# Definition of a Business Case

- *“A document used to justify the commitment of resources to a project”*
- *“Basis on which management will prioritise and decide whether to give the go ahead to a proposed Project”*

# A Better Definition...

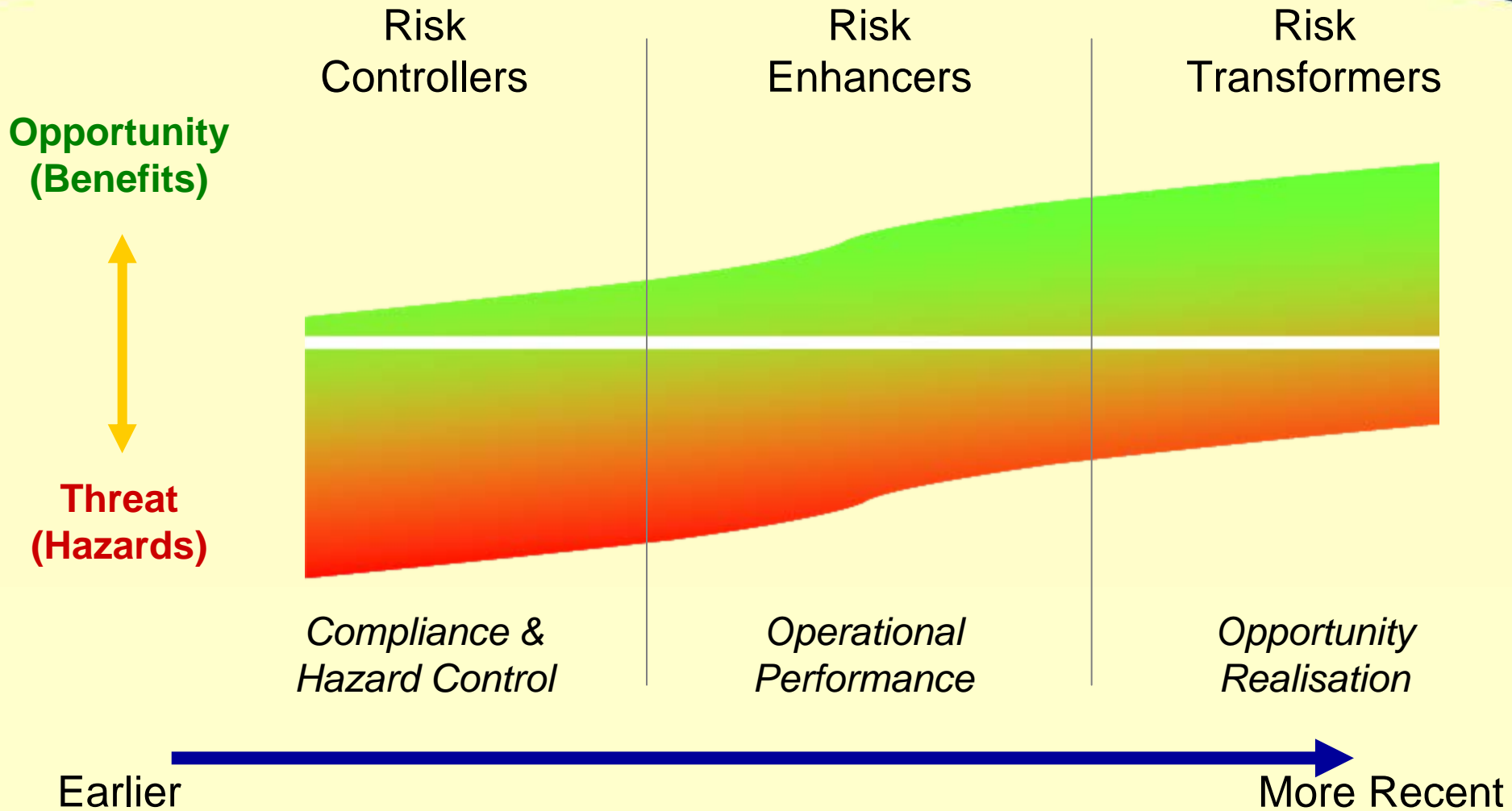
- *Provide the necessary financial projections, business metrics, and assessment of contingencies and risks, to support or reject business decisions.*



# 8 Simple Business Case steps...

1. What is the problem?
2. Why is it a problem?
3. What causes the problem?
4. What are the possible fixes?
5. What is the best fix (or fixes)?
6. Why is it the best fix?
7. What do we recommend to implement it?
8. What questions do we need to consider?

# Threat and Opportunity



# SRM Maturity Model

## **Level 4 - OPTIMISING**

*Proactive SRM, resilience & opportunity realisation practiced at all levels as part of competitive advantage*

## **Level 3 - REPEATABLE**

*Structured SRM built into routine management processes with evident awareness of benefits at all levels*

## **Level 2 - BASIC**

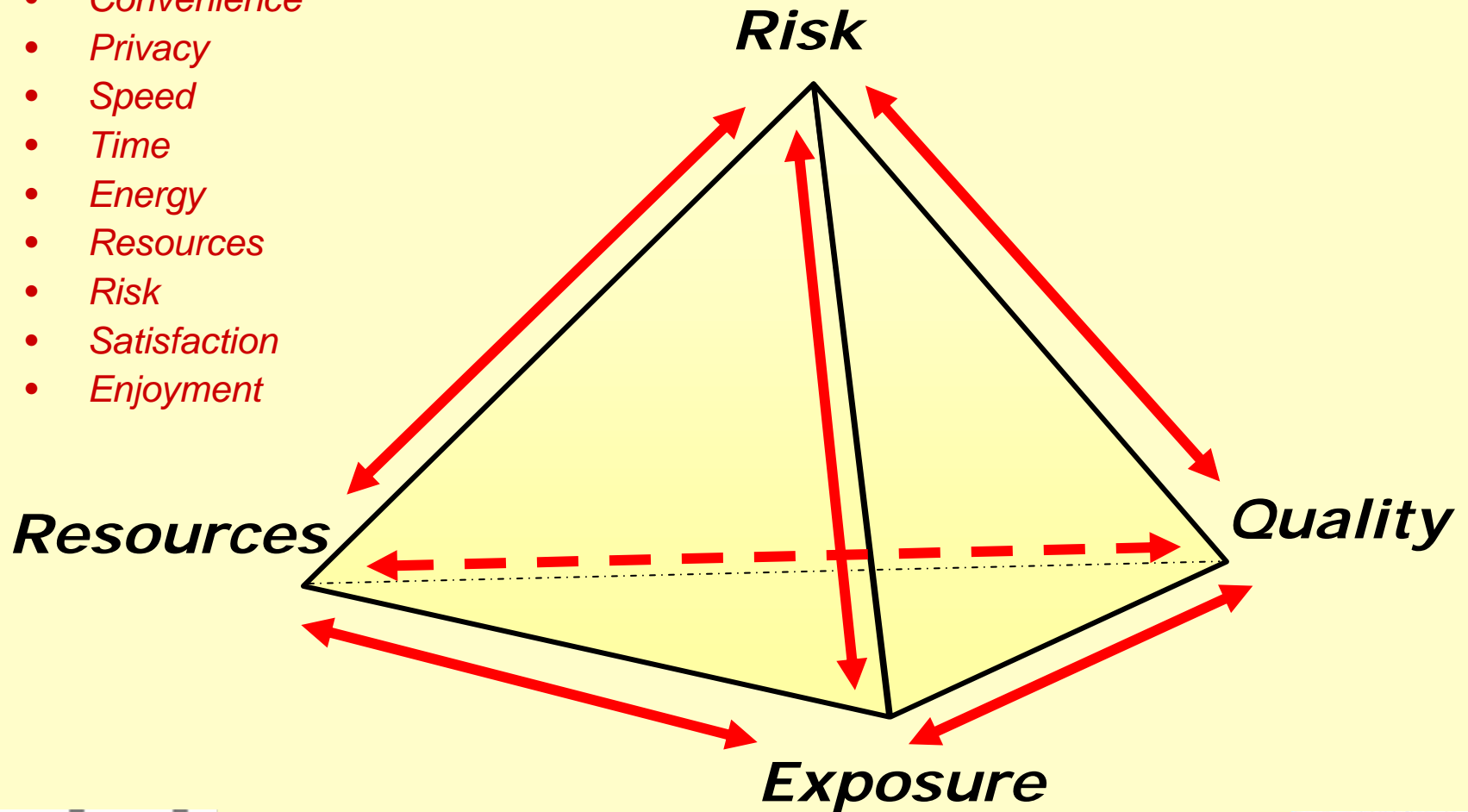
*Informal or unstructured SRM systems which are focussed on loss prevention and threat mitigation*

## **Level 1 - INITIAL**

*Compliance approach with minimal or excessive ad hoc reactive practices, and little awareness of SRM benefits*

# Security = trade-offs...

- Money
- Convenience
- Privacy
- Speed
- Time
- Energy
- Resources
- Risk
- Satisfaction
- Enjoyment



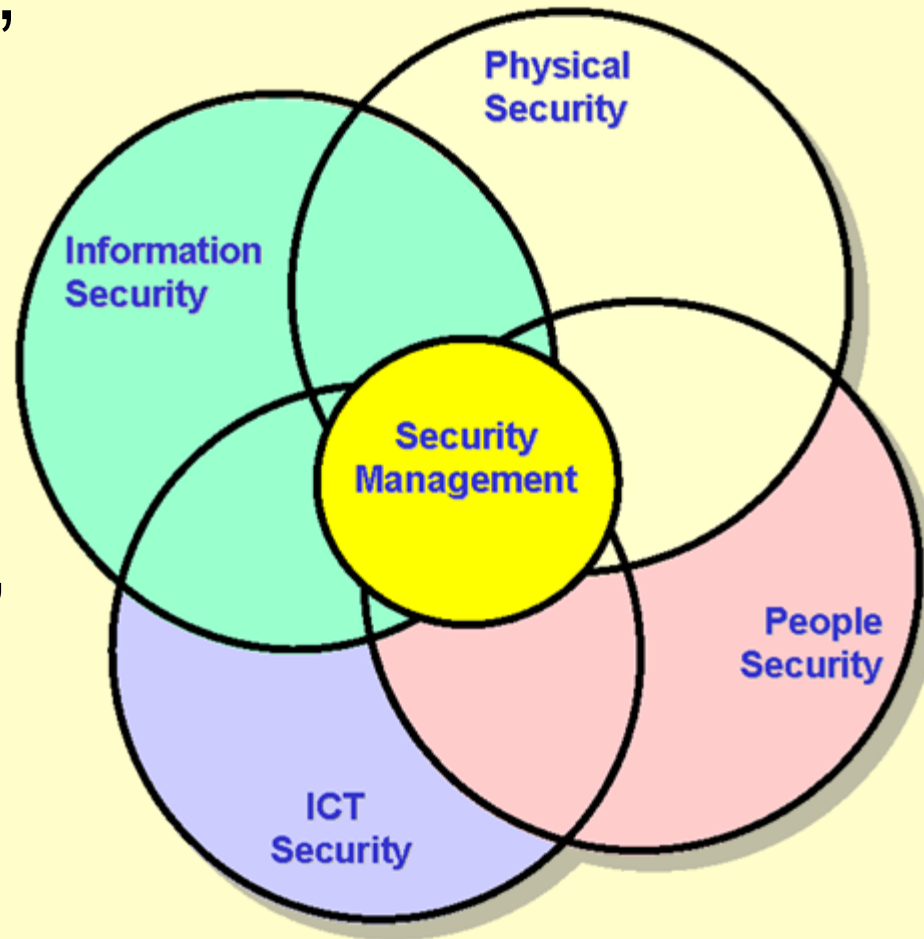
# Human-system Integration In System Development

1. 'Satisficing' requirements of stakeholders (buyers, developers, designers, users)
2. Incremental growth of system definition and stakeholder commitment
3. Iterative system definition & development
4. Concurrent system definition & development
5. Management of project risk

Source: National Academy of Sciences. <http://www.nap.edu/catalog/11893.html>

# Collaboration and Integration

- Senior Management, HR, Security, IT, maintenance, OHS procurement, and Risk Departments
- Main focus on business integration, enterprise security and value creation



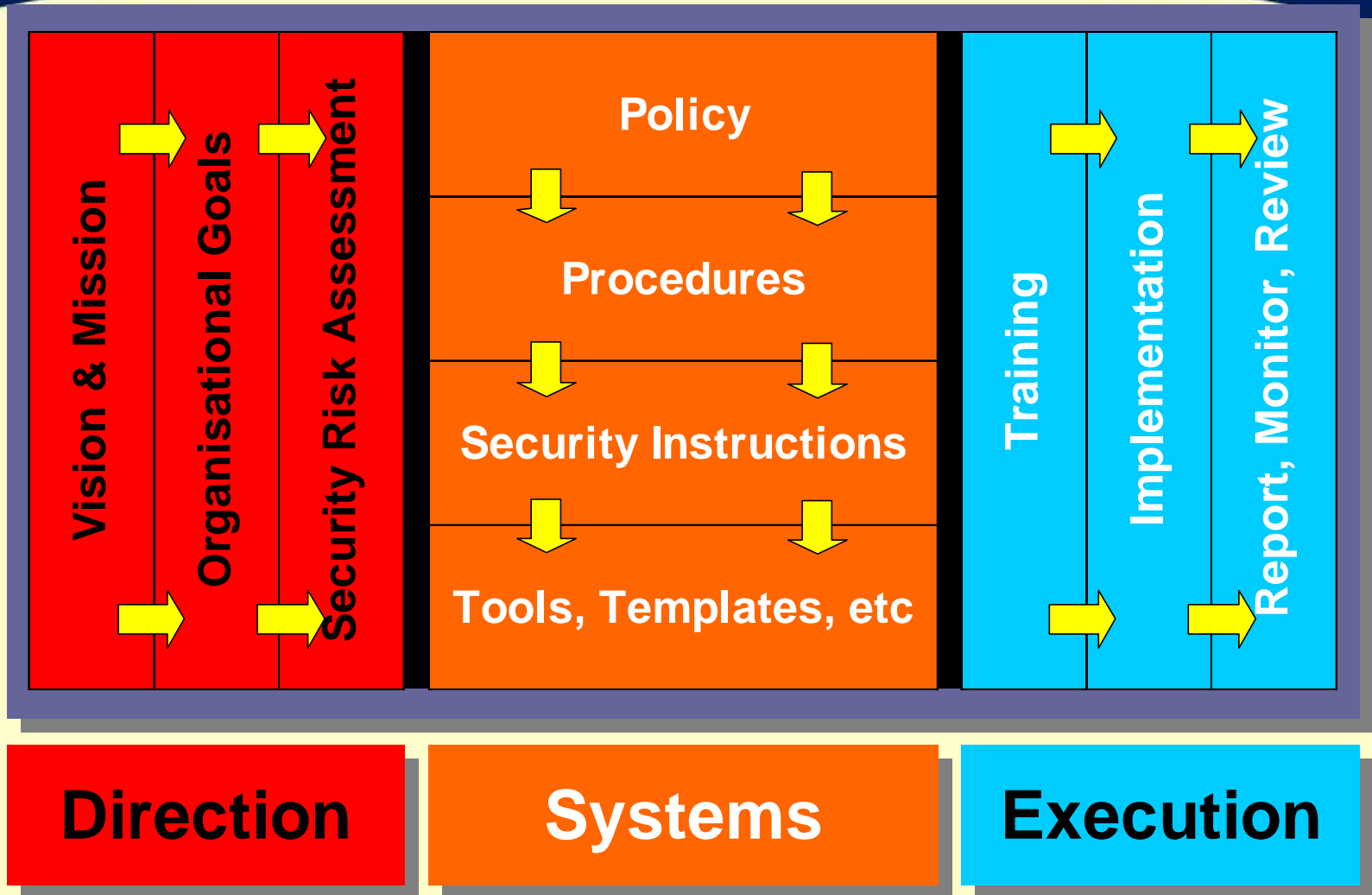
# Operating Priorities

1. Safety and Security
2. Doing business
3. Maintain infrastructure & systems
4. Improve...

# Operating Priorities



# Application



# Enterprise Security Standards

		THREAT LEVELS				
		1	2	3	4	5
<b>Intruder Alarm System</b>	VC	S	M	M	M	M-Crypt
	IMG		S	M	M	M-Crypt
	PMV		S	M	M	M-Crypt
	Esp.	S	M	M-Crypt	M-Crypt	M-Crypt
<b>Window Treatments</b>	VC	S <sup>1</sup>	S <sup>2</sup>	2343-R1	2343-R2	2343-R2
	IMG		S	2343-R1	2343-R2	2343-R2
	PMV		S	2343-R1	2343-R2	2343-R2
	Esp.		S	S	M	2343-G0
<b>Locks</b>	VC	M	M	M <sup>10</sup>	M <sup>11</sup>	M <sup>12</sup>
	IMG	M	M	M <sup>10</sup>	M <sup>11</sup>	M <sup>11</sup>
	PMV	M	M	M <sup>10</sup>	M <sup>11</sup>	M <sup>11</sup>
	Esp.	M	M	M <sup>10</sup>	M <sup>11</sup>	M <sup>12</sup>

Example Only

10 Pick-resistant hardened

11 Pick-resistant hardened, controlled profile

12 Pick-resistant hardened, restricted profile, organisation-endorsed

# Implementing Proactive SRM

- Barriers to understanding
- Guiding principles
- Application



# Barriers to Understanding

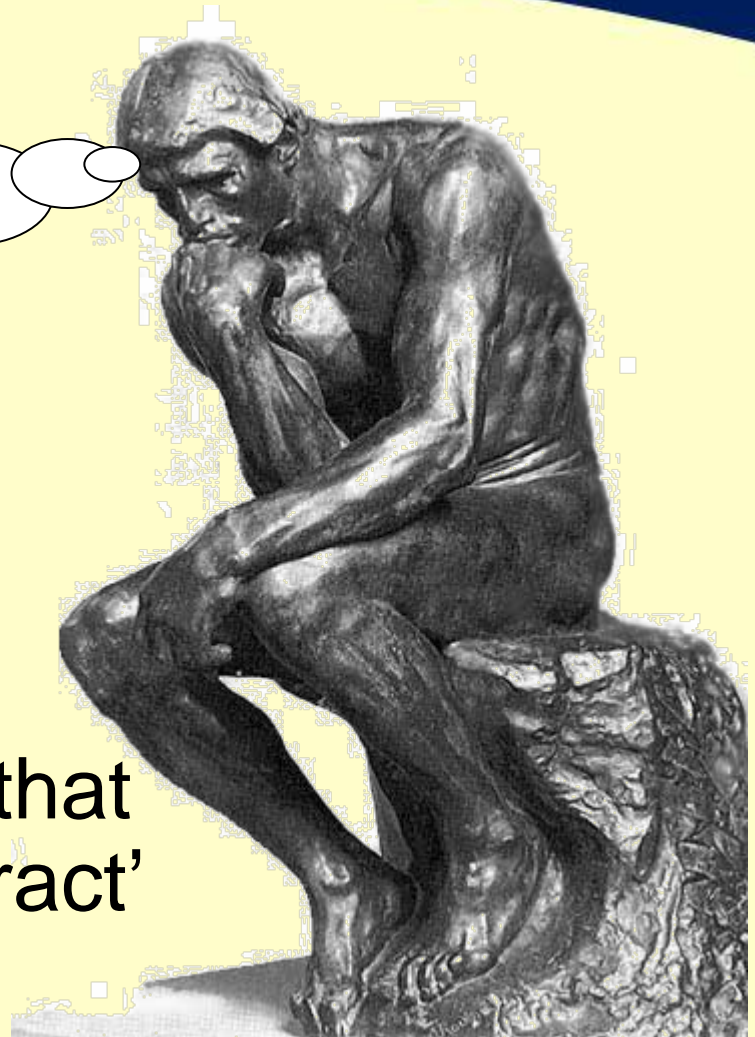
- Russian Roulette
  - 1 bullet
  - 6 chambers
- Life
  - 100 'bullets'
  - 6 billion chambers



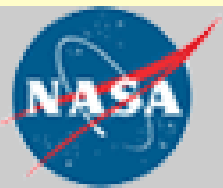
# A very abstract concept...

*“Expect some ingratitude from warnings about anything abstract...”*

- By definition, anything that did not happen is ‘abstract’



# Some Guidance from HRO's



NATIONAL AERONAUTICS  
AND SPACE ADMINISTRATION

# HRO's & 'Mindfulness'

- 1) Preoccupation with failure
- 2) Reluctance to simplify interpretations
- 3) Sensitivity to operations
- 4) Commitment to resilience
- 5) Deference to expertise

# Failure is rare in HRO's

## How do they learn?

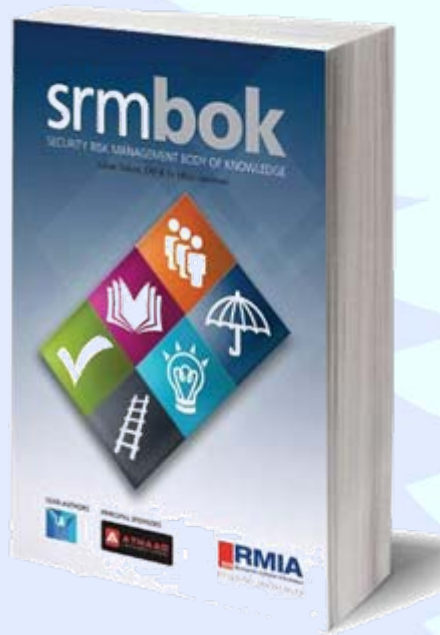
- 1) Capitalise on Rare Occurrences
- 2) All failures are windows on system health
- 3) Focus on the liabilities of success
- 4) Never forget that “*small moments of inattention can turn into unmanageable trouble*”
- 5) Thoroughly analyse near-miss events

# A Culture of Reporting...



# Key Challenges for SRM

- Limbic **AND** Neocortical regions
- Understand Problem/Benefit(s)
- ‘Mindfulness’
  - Pre-occupation with failure
  - Reluctance to simplify interpretations
  - Sensitivity to operations
  - Commitment to resilience
  - Deference to expertise
- Incremental Commitment Model



Thank you

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

[www.srmbok.com](http://www.srmbok.com)

# Intellectual Property Rights and Copyright

These slides and graphics are provided for public and corporate use to assist in consistency of presentation. They may be used on the following basis:

- Use of the material must acknowledge and identify Julian Talbot as the presentation developer or SRMBOK, RMIA, JBS as providers of the SRMBOK materials and/or where separately noted, other respective copyright owners.
- The material may be distributed to others as needed for the purpose of research as permitted under copyright legislation.
- The material is provided on an "as is" basis. without warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties of merchantability or fitness for a particular purpose.
- Information on SRMBOK procedures with respect to rights in RMIA and JBS specifications can be found at [www.srmbok.com](http://www.srmbok.com). Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification, can be obtained from [president@rmia.org.au](mailto:president@rmia.org.au).
- More information can be found at [www.jakeman.com.au](http://www.jakeman.com.au), [www.rmia.org.au](http://www.rmia.org.au) or by contacting [julian.talbot@jakeman.com.au](mailto:julian.talbot@jakeman.com.au).