



# **CHEIA Conference**

## **Assurance Mapping**

### **September 2012**

James C Paterson

Director, Risk & Assurance Insights Ltd.

These slides have been developed for the exclusive use of those attending the CHEIA annual conference by James Paterson, Risk & Assurance Insights Ltd.

This presentation has been prepared solely for educational and illustrative purposes. Whilst every effort has been made to ensure the factual accuracy of the content herein, no representation or warranty is given as to its accuracy.

This presentation should not be relied upon as the basis for making any investment or other decision and it is not claimed that any of the content or views contained herein, whether expressly made or implied, represents the views of management.

The slides should not be reproduced or circulated further without permission from James Paterson:

E-mail: [jcp@riskai.co.uk](mailto:jcp@riskai.co.uk)

Website: [www.riskai.co.uk](http://www.riskai.co.uk)

Mobile: +44 (0)7802 868914

“At the moment there is a sense in which assurance simply happens.

“It is not a planned activity in the way .. most IA departments.. prepare an annual plan. .

There is rarely an overall, documented plan for the totality of assurance that is required at the board level.”

Other  
Assurance

Internal  
Audit

Finance

Risk

Compliance

Board

Senior  
Management

## To reinforce this..

708 In order to assess the requirements for resources and funding for assurance purposes, the board should annually prepare or update an assurance map which should as a minimum:

- Document the people to whom assurance is required to be provided (eg regulators, investors, customers and so on), the nature of the assurance, how that assurance is to be provided and how the board is going to satisfy itself that the assurance that is being provided is truthful, correct and appropriate in all the circumstances.
- Document the manner in which the board will seek and obtain assurance that what they are told is happening in respect of the business is indeed happening in order to discharge the assurance aspects of their Corporate Governance duties to exercise risk management oversight.
- Document the way in which the board is assessing, monitoring and managing the risk management culture, and progress towards becoming a risk intelligent organisation

# From....

Other Assurance



Internal Audit

Finance

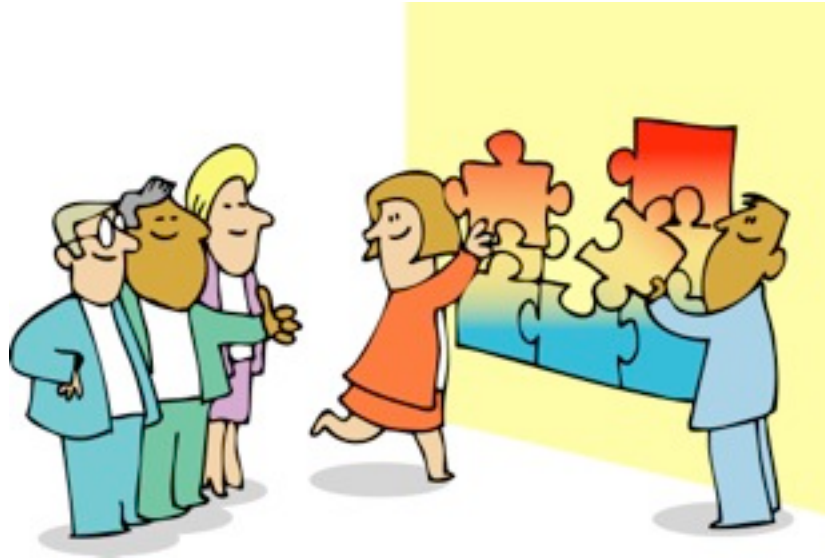
Risk

Board

Senior Management

Compliance

To....



Other Assurance

Internal Audit

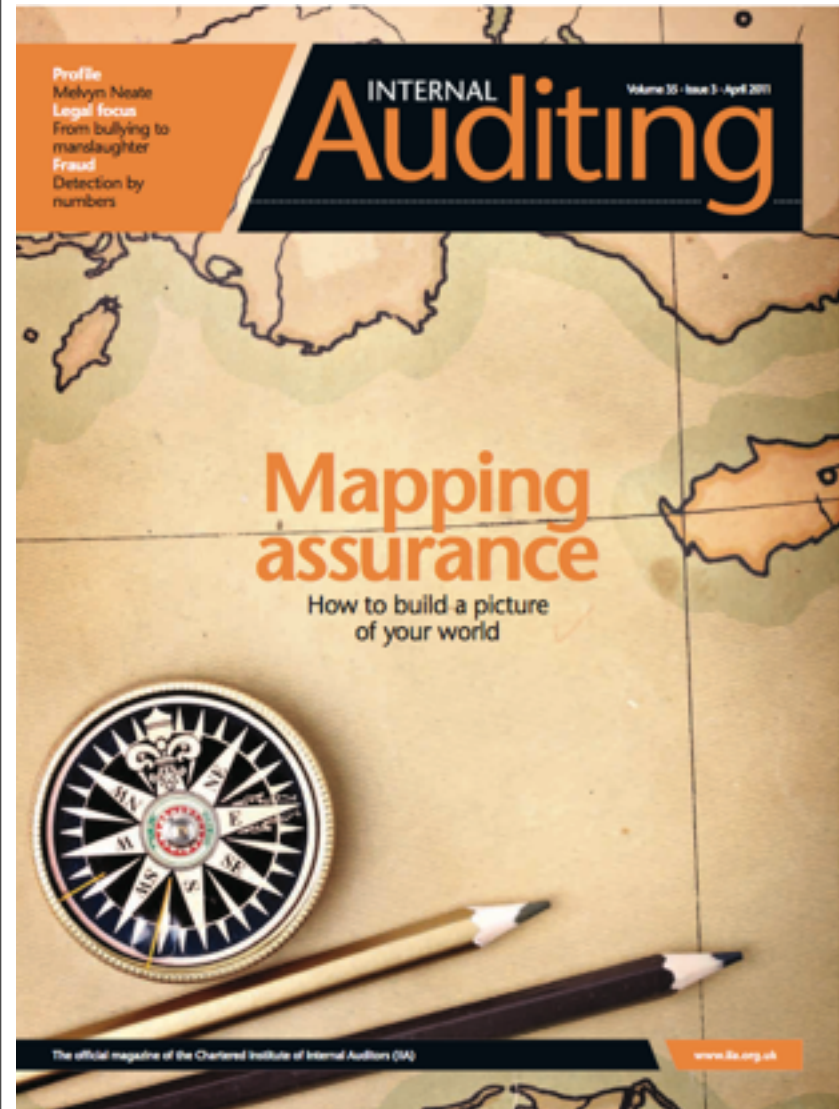
Finance

Risk

Board

Senior Management


Compliance



Power in this way of thinking

Many ways to slip up!

More uses than you might think



## Assurance : Definition

- ✧ A statement or indication that inspires confidence
- ✧ A guarantee or pledge
- ✧ Freedom from doubt; certainty





## What is an assurance map?



**IIA – 2050–2 July 2009, with some tweaks!**

An assurance mapping exercise involves mapping assurance coverage against **the key risks** in an **organisation**...

The aim is to ensure there is a comprehensive risk and assurance process with **no duplicated effort or potential gaps... to give stakeholders comfort..**

To understand where **overall risk and assurance roles and accountabilities** reside..

**Assurance from line management is fundamental** and should be complemented .. by assurance from IA and .. others..



## What is assurance?: Taking it on trust

as controls. However, in no case was it clear exactly how these controls might mitigate the risk effectively. The existence of a policy or strategy is really just a corporate statement of intent and says nothing about its implementation. Similarly, the existence of a committee is not in itself a control. The committee needs actively to monitor the action plan associated with a particular risk.

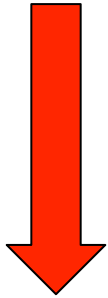
# AMAP Before

Risk area	1 <sup>st</sup> line	2 <sup>nd</sup> line	3 <sup>rd</sup> line
Legal risk	?	Management of key issues	N
Financial controls	Y	Reconcilliations, reviews and checks by some finance staff	Y – IA Y - EA

# AMAP After

Risk area	1 <sup>st</sup> line	2 <sup>nd</sup> line	3 <sup>rd</sup> line
Legal risk	Y	Clearer Overview Role agreed	Some IA reviews
Financial controls	Y	Building on current good practices, formalize finance control checks	Y- EA IA- Focussed reviews

# A critical question - Which risks? Why?



Risk area	Gross Risk	1 <sup>st</sup> line	2 <sup>nd</sup> line	3 <sup>rd</sup> line	Net Risk
abc	..	..	...	...	...
bcd	..	..	...	...	...
Cde	..	..	...	...	...
def	..	..	...	...	...
efg	..	..	...	...	...

# You have choices ~ ensure these are clear/agreed!

Current key risks



All risks / processes across the organisation

Compliance & Regulatory risks



Specific risks

- Finance
- IS/IT
- Treasury
- Business continuity

# Benefits delivery – Grander

Framework for risk accountability & assurance

Assurance on Current key risks

CRSA  
Incident reporting



Assurance there are “no risk black holes”

Improved sharing of risk, governance & controls load  
Across the 3 lines

More robust risk process / assessment

## Benefits delivery – more modest

Assurance a specific Risk or risk category is being assured

Streamlined Exec & Aud Co reporting

Improved sharing of specific accountabilities



Lean auditing

Synergies between Assurance functions

Co-ordinated “Audit” visits



# Too many benefits – confused / diffuse outcomes

Assurance on specific accountability  
& Risk or risk category  
is being assured

Assurance on  
Streamlined Exec &  
Aud Key reporting

CRSA  
Improved sharing of  
Incident reporting  
specific accountability



Assurance there are  
“no risk black holes”

Improved sharing of risk,  
governance & controls load  
Across the 3 lines

Synergies between  
More robust risk  
Assurance functions  
process /  
assessment

Co-ordinated  
“Audit” visits

# Case study


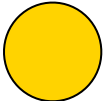



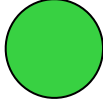
- ❑ Too many papers to Audit Committee
- ❑ Some assurances not being received
- ❑ Agree to agree top risks and develop scorecard




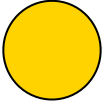
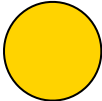
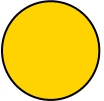



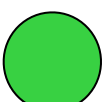

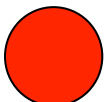

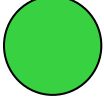


# Case study 4

# Key risks assurance scorecard - Q1 12

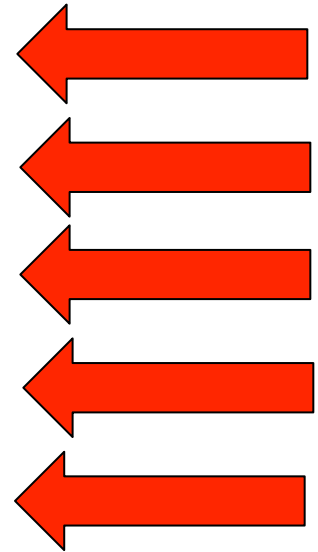
	Q1	Q2	Commentary
Student experience			No concerns from surveys
Funding			Finance Director satisfied
Government returns			Past issues about data quality being addressed by ....
Major projects			Steering Committees satisfied with progress
Points based immigration			Key managers report no issues of concern
Financial Controls			Financial controller satisfied

# Key risks assurance scorecard - Q2 12

	Q1	Q2	Commentary
Student experience			Latest surveys show some slippage in ratings ~ report on action plan progress at the next board meeting
Funding			Fee increases affecting applications, being watched closely by the Finance Director
Government returns			Improvements in hand to ensure high quality government returns
Major projects			No issues being reported from Steering Groups, Executive review of key plans in Q3 12
Points based immigration			Newspaper coverage / Internal Audit review suggests weaknesses that could cause reputational damage
Financial Controls			No issues from Financial Controller, External Auditor due to review in Q3 12

# Who is accountable for what?

Risk area	Gross Risk	1 <sup>st</sup> line	2 <sup>nd</sup> line	3 <sup>rd</sup> line	Net Risk
abc	..	..	...	...	...
bcd	..	..	...	...	...
Cde	..	..	...	...	...
def	..	..	...	...	...
efg	..	..	...	...	...



**Accountabilities:**  
“Success – I did it”



# Accountabilities

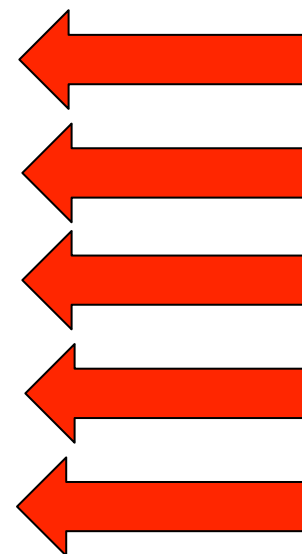
“Failure – it was their fault”





# Who is accountable for what?

Risk area	Gross Risk	1 <sup>st</sup> line	2 <sup>nd</sup> line	3 <sup>rd</sup> line	Net Risk
abc	..	..	...	...	...
bcd	..	..	..	...	...
Cde	..	..	...	..	...
def	..	..	...	...	...
efg	..	..	...	...	...



- If this is unclear you will have problems!
- Specific risks ~ Information Security / Projects
- Generally ~ Line management / Policy functions
- HE context ~ Government returns / Immigration points based system?

# Any AMAP must pay close attention to Accountability

Current key risks



All risks / processes across the organisation

Compliance & Regulatory risks



- Specific risks
- Finance
  - IS/IT
  - Treasury
  - Business continuity

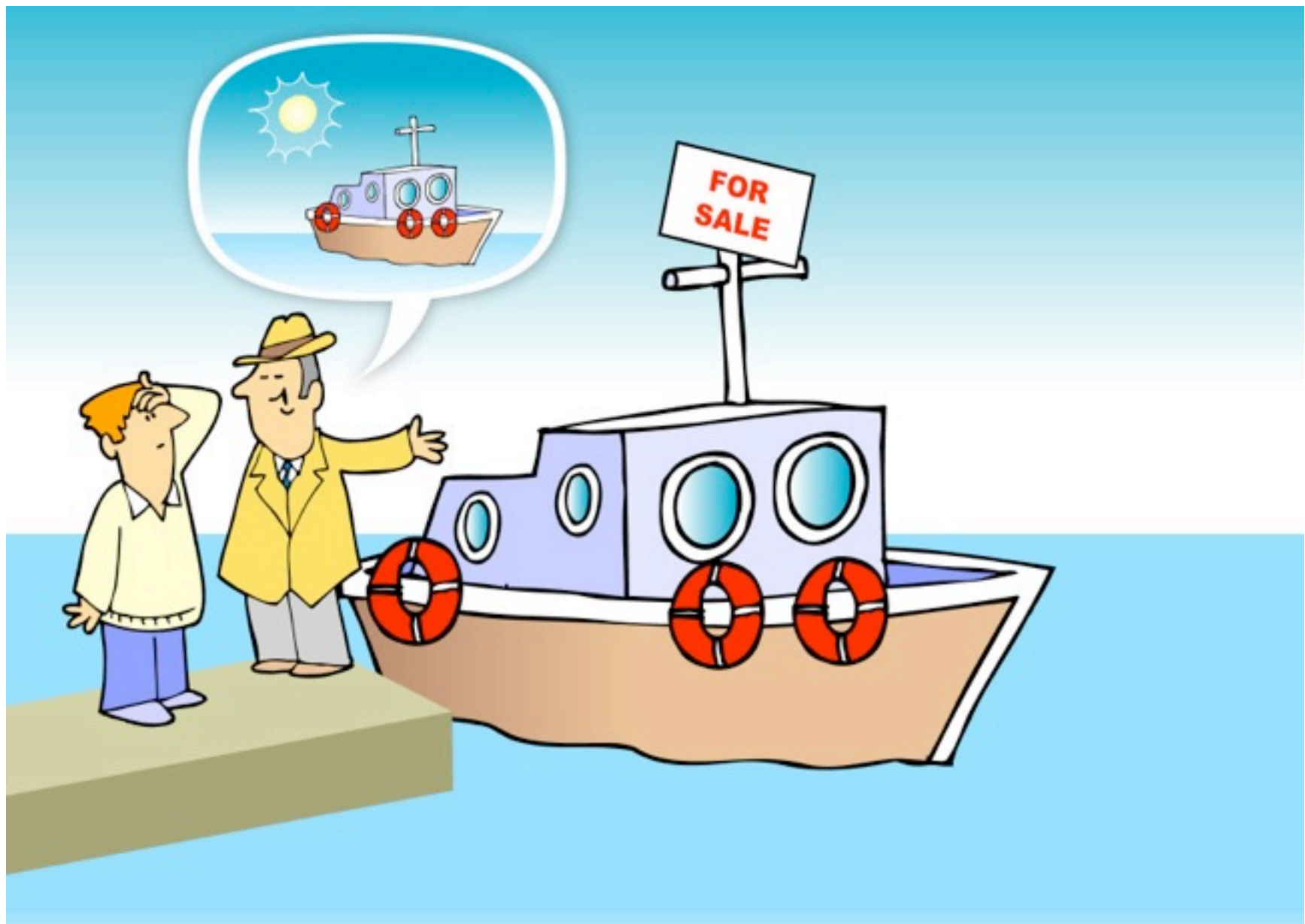
**How many accountability questions do you want to open up?  
Need to use tools such as RASCI**

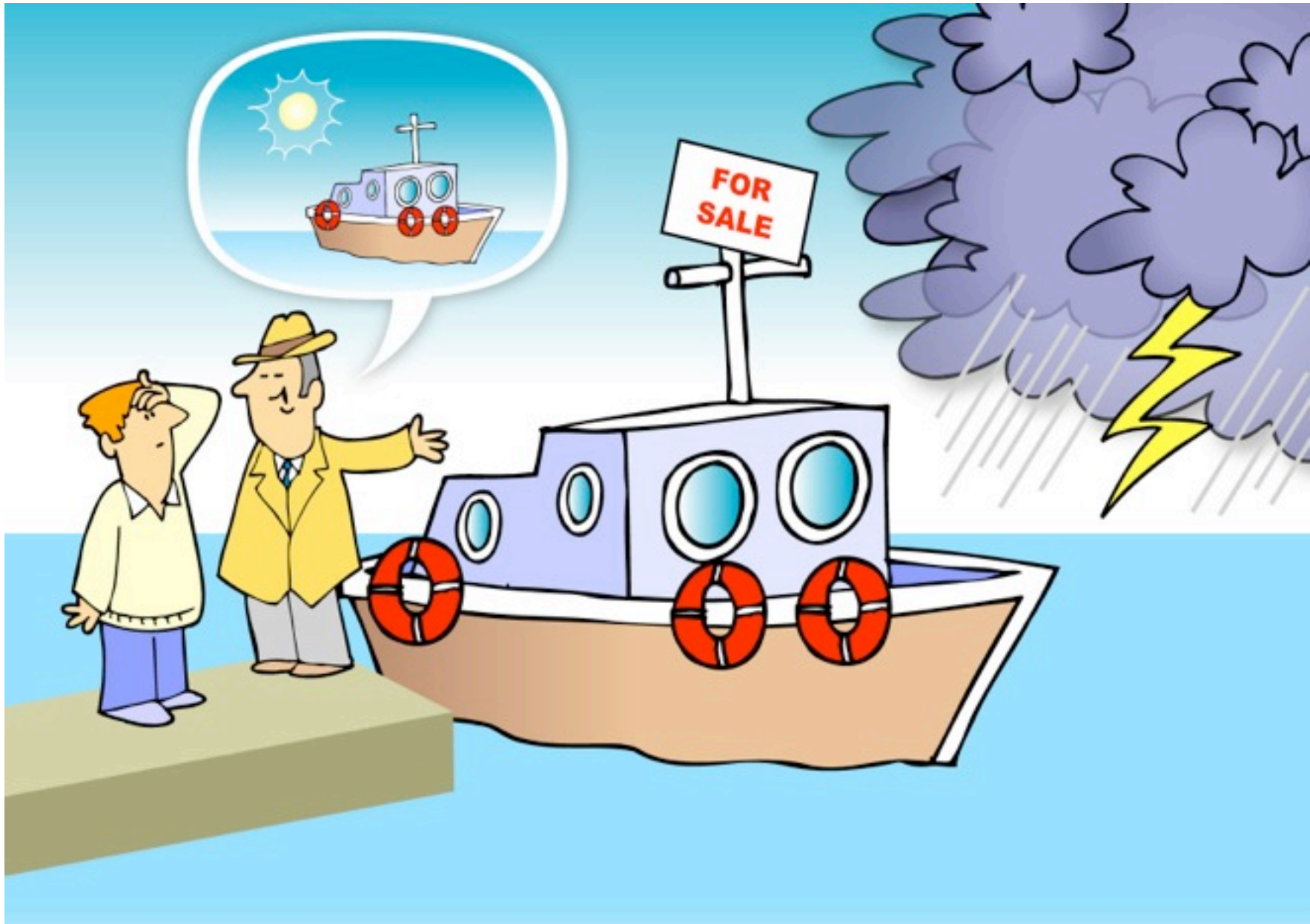
# Even if accountabilities clear ~ what level of assurance?

Risks	Key control A	Key control B	Key control C	Other control	Other control
Key risk 1					
Key risk 2					
KR3					
OR					
OR					

Or this?

Risks	Key control A	Key control B	Key control C	Other control	Other control
Key risk 1					
Key risk 2					
KR3					
OR					
OR					





# The question of depth

**Consider depth / breadth explicitly**

~ when seeking assurances

~ when carrying out audits

**Can be helpful to think about Key risks & Key controls**

**Sharpen IA & organizational understanding of these**



# The question of depth / breadth

## Depth

Review

Audit

Investigation

## Breadth

Focussed

Key risks

Comprehensive



# The question of risk appetite

**Consider explicitly for key risks**

**Hungry**

**Open and aware**

**Cautious**

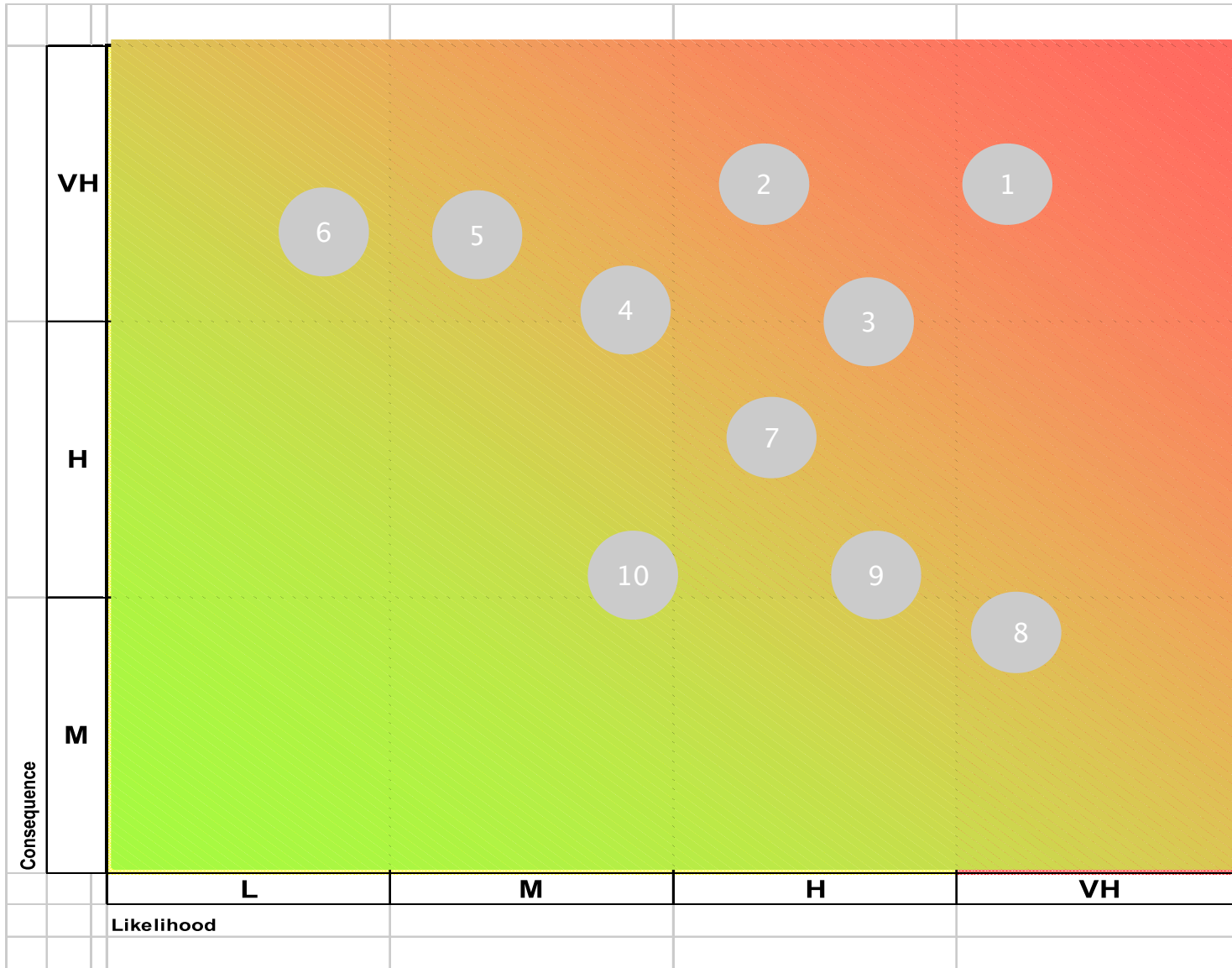
**Averse**





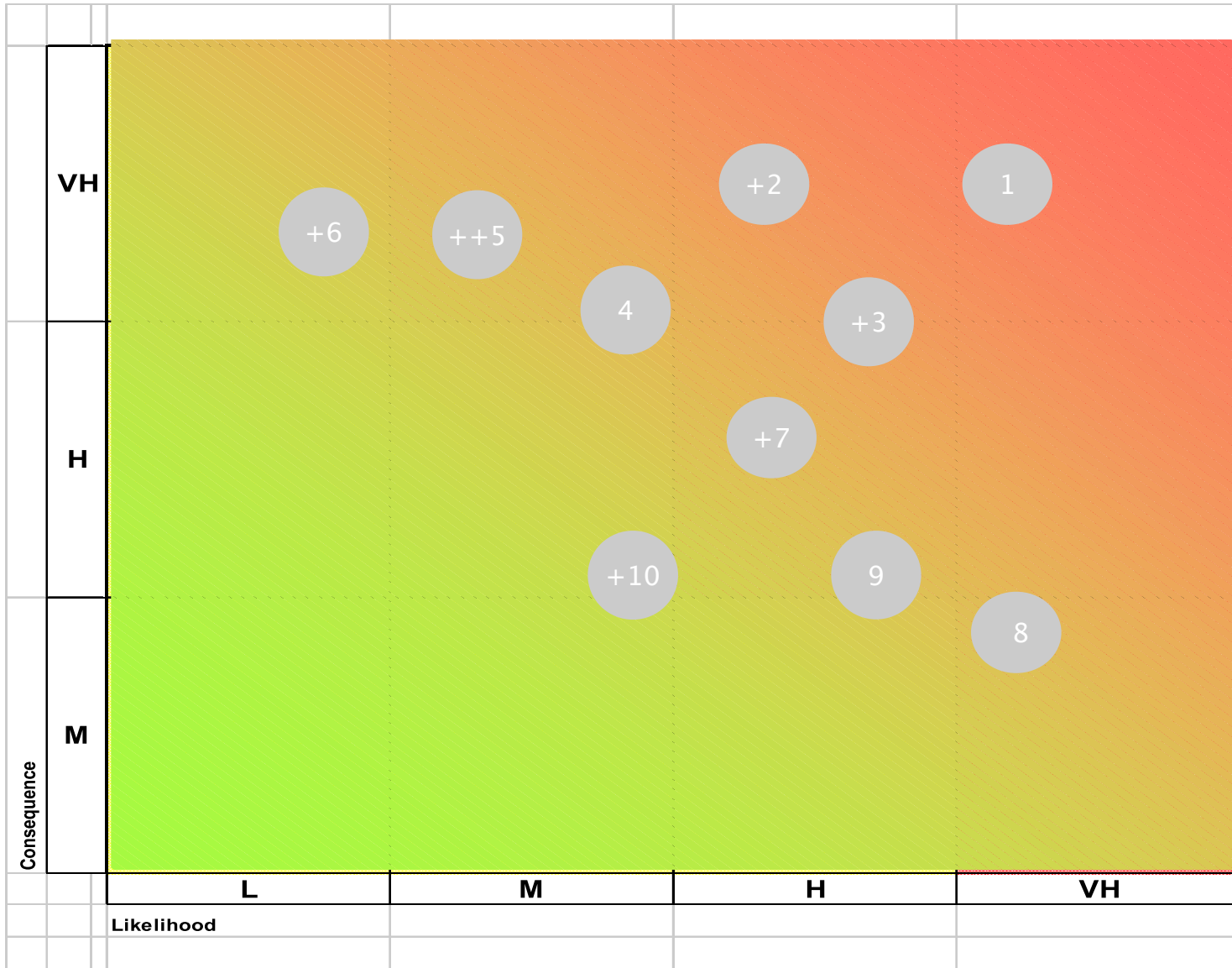
# Looking at an audit plan

# Look at top risks



- 1 - Student Experience
- 2 - Funding
- 3 - Govt Returns
- 4 - Major Projects
- 5 - Financial controls
- 6 - Points based immigration

# Capture Other Assurances + (some ) or ++ (lots)



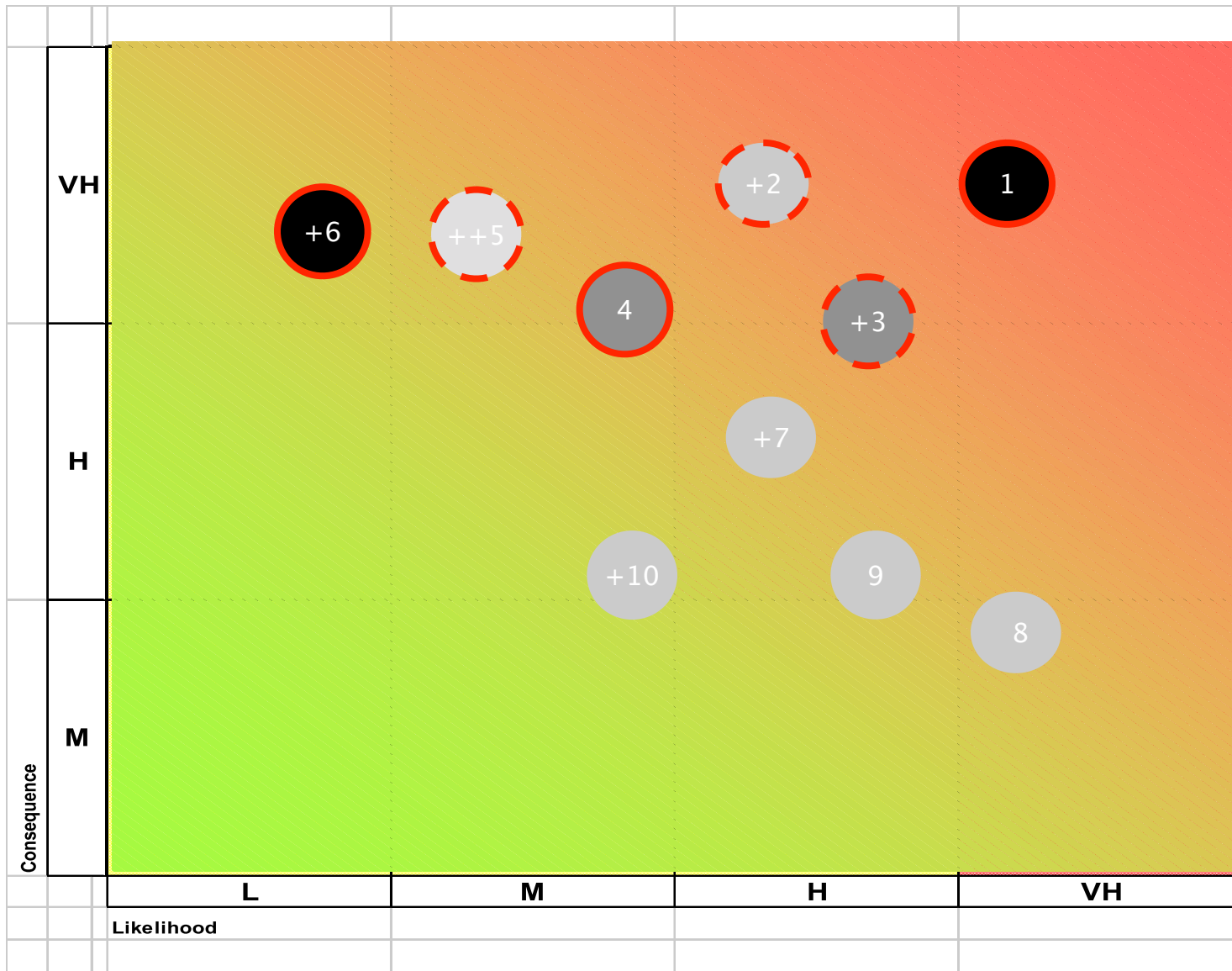
- 1 - Student Experience
- 2 - Funding
- 3 - Govt Returns
- 4 - Major Projects
- 5 - Financial controls
- 6 - Points based immigration

# Robustness of assurance ~ factors to consider

- the independence of the reviewer;
- the frequency of their review;
- the timeliness of reporting on completion of fieldwork;
- the scope of the review;
- how much evidence was reviewed during the review;
- whether reports include action plans and are followed up by the reviewer;
- the skills and status of the reviewers; and
- whether the output includes opinion on adequacy of controls in place.

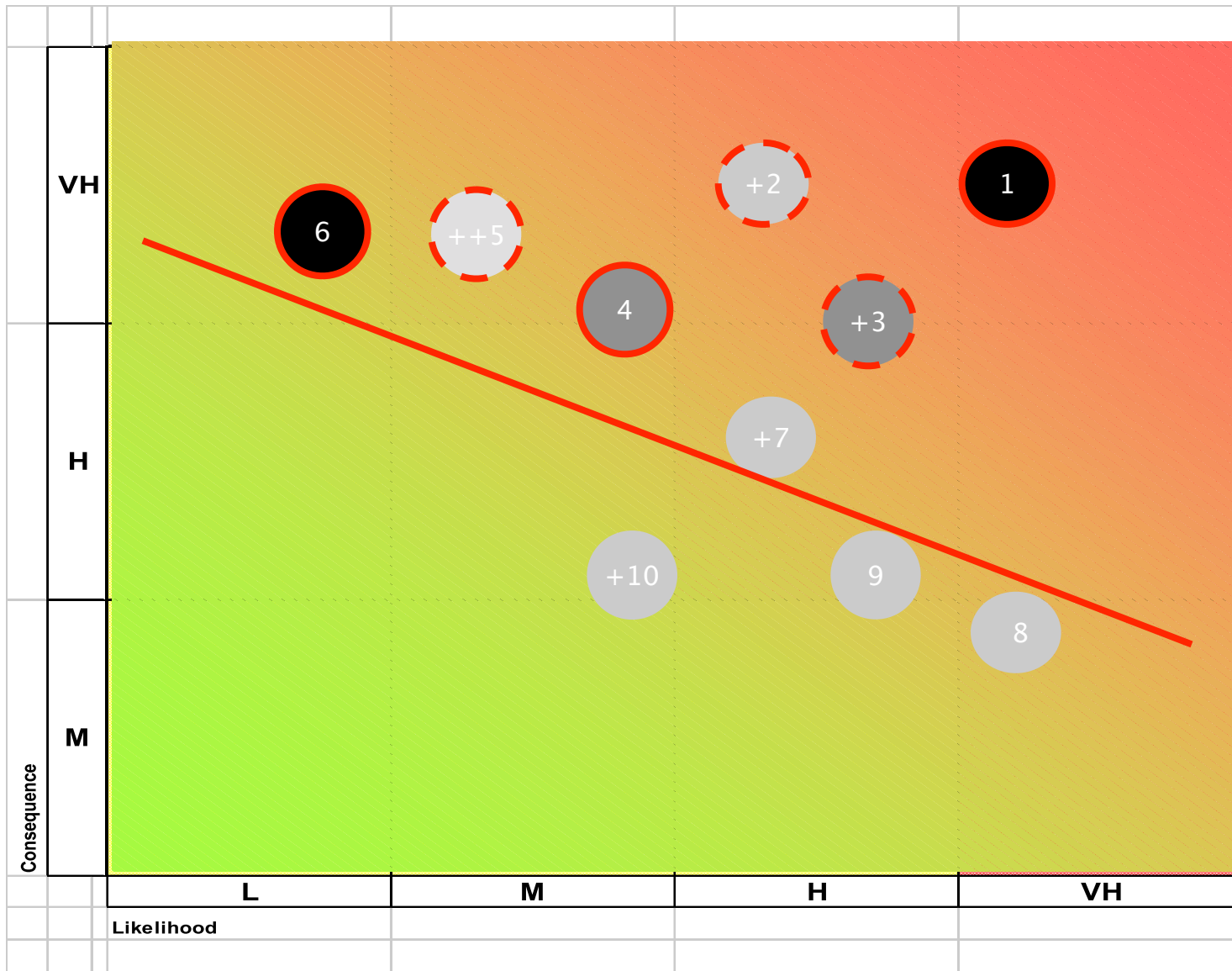
**Do NOT rush to criticise / stop weaker assurance**

# Past coverage ~ colour of risk



- 1 - Student Experience
- 2 - Funding
- 3 - Govt Returns
- 4 - Major Projects
- 5 - Financial controls
- 6 - Points based immigration

# Proposed plan: Solid red ~ audit; dotted red ~ review



- 1 - Student Experience
- 2 - Funding
- 3 - Govt Returns
- 4 - Major Projects
- 5 - Financial controls
- 6 - Points based immigration



# Plan example ~ Fraud

AUDIT AREA	BACKGROUND	MANAGEMENT OVERSIGHT	PROPOSED COVERAGE & RATIONALE
Fraud risk	In the current economic climate, this is an area for vigilance. The amounts at risk may not be significant, but should not be neglected	A range of functions will ensure, through prevention and detection controls, that frauds are not committed on a day to day basis: Finance, Purchasing, Payroll etc.	We will carry out a <u>high level review</u> , identifying those areas that are potentially most susceptible to fraud  We will then carry out further targeted work including the use of Computer Aided Audit Techniques, which are commonly deployed in functions such as Purchasing, Payroll and Travel & Expenses.

## Tip ~ show equivalent cycle times across all areas

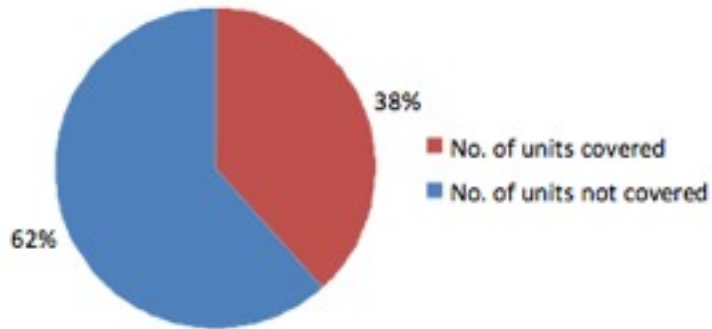
	IA resource in this year		Cycle time implications
	Audit	Advice	
Financial Controls	20	-	1 / year
Compliance	30	5	1 / 2 years
Operational Controls	15	10	1 / 3 years
Strategic risks	5	5	1 / 8 years
<b>TOTAL</b>	<b>75</b>	<b>25</b>	



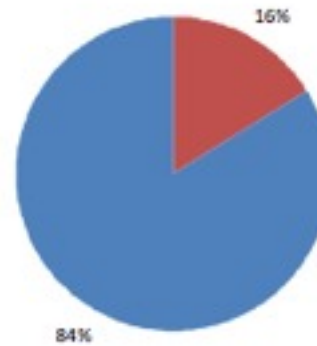
# Coverage by areas of more / less significance

## Proposed FY13 Coverage by location

Tier 1<sup>1</sup>



Tier 2



Tier 3



## **“Taking it on trust” ~ Findings**

- greater attention needed to be paid to compliance mechanisms and these needed to be more clearly distinguished from internal audit, which should review the effectiveness of the compliance framework, not be a substitute for it;

# Information Quality

## ~ Department / Risk theme analysis

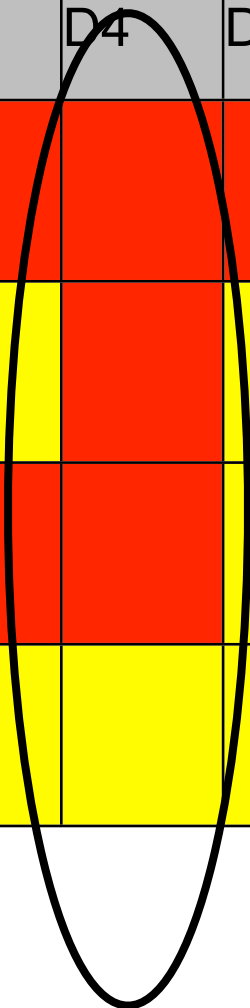
	D1	D2	D3	D4	D5	D6	D7	D8	D9
Fin impact									
HEFCE sensitivity									
Ext impact									
Concerns									

# Assessment of importance of info quality

	D1	D2	D3	D4	D5	D6	D7	D8	D9
Fin impact	Red	Red	Red	Red	Red	Red	Yellow	Yellow	Yellow
HEFCE sensitivity	Red	Red	Yellow	Red	Yellow	Yellow	Yellow	Green	Green
Ext impact	Red	Yellow	Red	Red	Yellow	Yellow	Green	Green	Green
Concerns	Green	Green	Yellow	Yellow	Yellow	Green	Green	Green	Green

# Information quality

	D1	D2	D3	D4	D5	D6	D7	D8	D9
Fin impact	Red	Red	Red	Red	Red	Red	Yellow	Yellow	Yellow
HEFCE sensitivity	Red	Red	Yellow	Red	Yellow	Yellow	Yellow	Green	Green
Ext impact	Red	Yellow	Red	Red	Yellow	Yellow	Green	Green	Green
Concerns	Green	Green	Yellow	Yellow	Yellow	Green	Green	Green	Green













# Information Quality assurance approach

Area	Staff	Manager	Other
Culture / Oversight			
Objectives / R&Rs			
Risk and mitigations			
Policies			
Develop policies, standards & training			
Implement standards & controls			
Monitoring			
Incident management & corrective action			
Auditing			

Consider for a department, w.r.t. data that really matters

# Information Quality assurance approach

Area	Staff	Manager	Other
Culture / Oversight			
Objectives / R&Rs			
Risk and mitigations			
Policies			
Develop processes, standards & training			
Implement standards & controls			
Monitoring			
Incident management & corrective action			
Auditing			



## Suitable description..

- ❖ Key risks vs. Value Chain: “A risk heat map”
- ❖ 1<sup>st</sup> line accountabilities map: “Senior Management accountabilities”
- ❖ Assurance coverage map : “Audit and compliance planning schedule”  
“Resource deployment schedule”
- ❖ Assurance map: “Assurance scorecard”  
“ Key risk status report”





## Assurance map ~ key points

- Scope / Purpose
- Which risks / controls
- Who is accountable?
- Assessment of assurance ~ Assessment of risks
- Mechanics of inputs and managing language differences
- Outputs linked to customer/stakeholder needs
- Culture and change management including an appropriate A-Map description
- Benefits ~ what / for who, including finding the right hook / quick win
- Embedding ~ Continuous improvement

## J Paterson: Publications / Citations


Topic	Publication	Month / Year
Internal Audit ~ New rock and roll	Accountancy Magazine, UK	January 2005
Forbidden Territory (auditing no go areas)	IA & BR UK	December 2006
Meeting the people challenge	IA & BR UK	February 2007
Garbage in, garbage out	Internal Auditor	June 2007
The power of prioritisation	Audit Director Roundtable	December 2007
Getting the most from your IA function	ACCA e-bulletin	June 2008
Lighting up your blind spots	IA & BR Magazine UK	March 2010
Mixed Messages	Strategic Risk Magazine	March 2010

# J Paterson: Publications / Citations

Topic	Publication	Month / Year
Know your business	Internal Auditor, US	June 2010
Help or hindrance?	Risk Management Professional	June 2010
A problem shared (Action Learning)	IA & BR Magazine UK	June 2010
Culture & behavior	IA & BR Magazine	March 2011
Assurance Mapping	CFO World	March 2011
Assurance Mapping	IA & BR Magazine UK	April 2011
Psychology of risk and audit	ACCA UK e-bulletin	June 2011
Lean Auditing	CIPFA Audit Viewpoint	August 2011
Lean Auditing	Audit & Risk W/S UK	September 2011

# J Paterson: Publications / Citations

Topic	Publication	Month / Year
HIA career paths	Symmetry	November 2011
Boards and Risk	Risk Management Professional, UK	December 2011
Audit Planning	<a href="http://theiia.org/chapters/500">theiia.org/chapters/500</a>	December 2011
New year new plan	Audit & Risk Magazine, UK	January 2012
Risk assurance and assurance mapping	CIPFA Audit Committee update	February 2012
Key performance indicators	IIA Denmark	April 2012
Coordinating assurance	Audit & Risk Magazine, UK	May 2012
Tips for new HIAs	Audit & Risk website	July 2012
Dear Audit Committee Chair	<a href="http://www.riskai.co.uk">www.riskai.co.uk</a>	September 12



These slides have been developed for the exclusive use of those attending the CHEIA annual conference by James Paterson, Risk & Assurance Insights Ltd.

This presentation has been prepared solely for educational and illustrative purposes. Whilst every effort has been made to ensure the factual accuracy of the content herein, no representation or warranty is given as to its accuracy.

This presentation should not be relied upon as the basis for making any investment or other decision and it is not claimed that any of the content or views contained herein, whether expressly made or implied, represents the views of management.

The slides should not be reproduced or circulated further without permission from James Paterson:

E-mail: [jcp@riskai.co.uk](mailto:jcp@riskai.co.uk)

Website: [www.riskai.co.uk](http://www.riskai.co.uk)

Mobile: +44 (0)7802 868914