Today's agenda

Warning: presentation contains one scene of nudity

1. Risk management background and context (6 slides)
2. Risk registers: the good bits + the non-technical bad bits (5)
3. Risk registers: probability-impact risk assessment (PIRA) (4)
4. PIRA in theory: dice, wave damage and a huge problem (7) ☹
5. PIRA in practice: specific issues arising (but hiding) (10)
6. Towards better risk assessment: double triangle prototype (5) ☺
7. Even better risk assessment: a few more suggestions (4)
8. Summary checklist and conclusions (2)

8 Appendices: (28 slides)
More detail, more curious/technical material, links and references.

WARNING: some of the authors in the references might affect your views on risk management

[0] Presentation objectives

- 3 types of presentation: 1: bad, 2: good but unusable later
- I want this one to be **3: good and helpful in the months to come**

- I will seek to show that risk registers:
  1. are doubly (and unnecessarily) subjective for risk assessment
  2. can mislead at reporting stage (because reporting is "lossy")
  3. offer a weak basis for decisions / action (due to insufficient information)
  4. often have little link to other (risk/non-risk) parts of the business

- For believers I'll offer hope:
  - A "double Δ" prototype (more science, easily extendable)
  - A summary checklist: "10 ways to get better"
  - 8 Appendices, including a host of references and links

- Appendix 1 confesses "where I'm coming from" (my bias)

[0] Interactive reality test

This is not a trick question...

- The summary claimed "no prior knowledge" was necessary
- Has anyone <u>not</u> seen one of these before? (Be brave!)

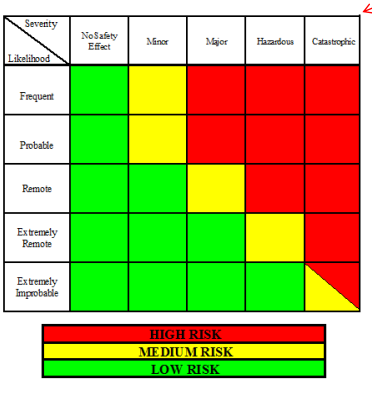


Figure 3 - 1. Predictive Risk Matrix

- Risk assessment in risk register
- Likelihood / severity
- ≈ Frequency / effect
- ≈ Probability / impact

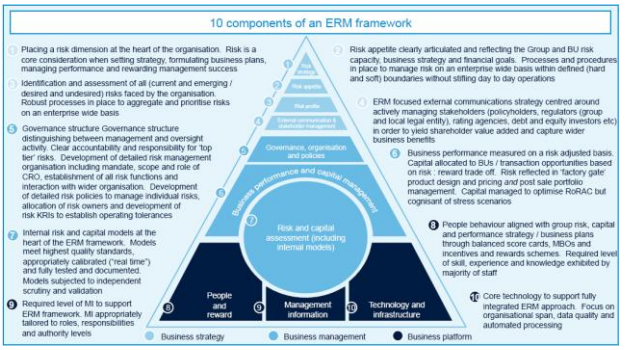
- Abbreviations:
  - RR = Risk register
  - PIRA = Probability / impact risk assessment

[0] Do risk registers matter?
... and what does that mean for today?

1. Who works in an organisation that uses a RR?
2. Who here has responsibility for maintaining a RR?
3. Who here has responsibility for reporting using a RR?
4. Who works where RRs are used to make decisions?

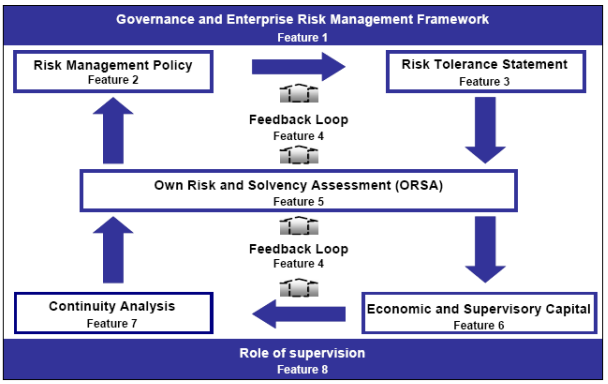
- (4) is key:
- If RR are used for decisions they should be “good”
- If they’re not used just stop.

[1] Risk management background and context
When you add on all the “overhead” RM is big



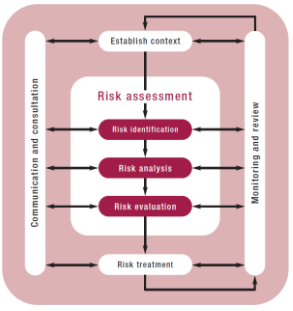
- A scary diagram(?) with a lot of “overhead”
- Quite “insurer-centric” e.g. two mentions of capital
- Risk assessment is core (item 7)
- Not obvious what you *do*

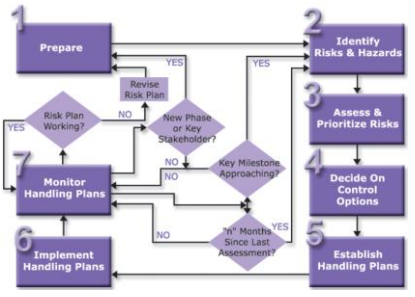
[1] Risk management background and context
Some may prefer a simpler version



- Risk and solvency / capital assessment is again core
- Source: IAA – see references

[1] Risk management background and context
Getting to the "doing" of risk management





- Source: LHS "A structured approach to ERM and ISO 31000"
- Source: RHS Mitre risk process. For both see references
- Questions such as "When does this process stop / start?" and "To what is the process applied?"... are "out of scope" for today

[1] Risk management background and context
What does a risk register look like?

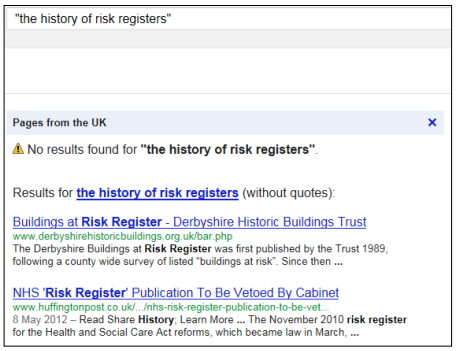
- Birthday party example from Wikipedia

Risk Category	Risk Name	Risk Number	Probability (1-3)	Impact (1-3)	Risk Score	Mitigation	Contingency	Action By	Action When
Guests	The guests find the party boring	1.1.	2	2	4	Invite crazy friends, provide sufficient liquor	Bring out the karaoke	Mack	within 2hrs
Guests	Drunken brawl	1.2.	1	3	3	Don't invite crazy friends, don't provide too much liquor	Call 911	Jerry	Now
Nature	Rain	2.1.	2	2	4	Have the party indoors	Move the party indoors	Milind	10mins
Nature	Earthquake or fire	2.2.	1	3	3	Start the party with instructions on what to do in the event of fire or earthquake	Implement the appropriate natural disaster response plan	Everyone	As per plan

- Mitigation would be better labelled controls (i.e. pre-crystallisation measures)
- Contingency sometime labelled mitigation (i.e. post-crystallisation measures)
- Sometimes have "gross", "net" (of controls) and "target" (for any or all of P, I or score)
- Often multiple controls against one risk, which can get messy

[1] Risk management background and context
The history of risk registers

[1] Risk management background and context
The history of risk registers



- COSO 1985
- Sponsored the Treadway Commission (fraud in accounts)
- Treadway originally jointly sponsored and funded by 5 main professional accounting associations
- Resulted in "Internal Control: Integrated Framework" (1992 and 94)
- Coopers & Lybrand wrote the report
- RRs have made their way into some (but not all) RM standards

✓ Can be "industrialised"

- RRs have little history compared to probability, models and science
- Little review of their actual effectiveness
- Having been involved in this, accounting firms pushed risk registers
- "Promoted by ... consultants and international standards organizations"

[2] Risk registers: some good bits
Admissions from a critic

1. **List of risks (worry list?)**
   - Identification then listing
   - Avoid reinvention of the wheel
   - Helps speed up risk assessment (etc)
2. **List of controls (wish list?)**
   - The heart of risk management
   - Without this it's just analysis
   - Risk-control matrix is a powerful concept (see Appendix 2)
3. **A checklist**
   - More a "to do" list than risks (risk assessment may be played down)
   - e.g. "deal" risk register (to an extent – a mix of "to do" and risks)
   - Flight checklist: mainly a reminder (we hope)

[2] Bad features: non-assessment aspects
At least how RRs are typically used

1. ERM claims a holistic treatment of risk but ...
   - ✓ Risks are treated holistically in that they pass through the same ERM framework and are presented consistently.
   - × A RR's PIRA-type risk assessment applies to individual risks
     - PIRA does not seek to quantify total risk and
     - PIRA makes no allowance for dependencies
     - See Appendix 8 for a striking zero correlation example
   - × RRs rarely consider/quantify "upside risks" in practice
2. Integration with the business. Weak links to:
   - Business model (e.g. key strategic aspects)
   - Financial models (e.g. appraisal value)
   - Capital quantification (completely separate exercise for most risk types)
   - Risk appetite / tolerance – instead a different scale is introduced

[2] Bad features: risk assessment aspects
At least how RRs are typically used

3. Problems with probability-impact risk assessment
   - a) Risks are (typically) poorly described
   - b) No allowance is made for known behavioural biases
   - c) Risk is seen as an event rather than a distribution
   - d) The PIRA methodology significantly worsens subjectivity
   - e) Assessments are "lossy" (multiple times for the same risk)
   - f) Assessments probably wrong?
   - g) Poor basis for decision making

- Presentation concentrates on c)-g)
- Other points are covered in Appendices 6 and 8

[2] Real world probability versus schooldays
"It's unfair to damn RR too badly"

1. Schooldays probability ("classical")
   - Techniques include symmetry, counting and "rules" of probability
   - Probabilities are known and don't change over time
2. Real world probability
   - Probabilities are (generally) unknown
   - There is often little or no relevant data (beyond "expert opinion")
   - Probabilities also change over time

- Risk registers need to meet the challenge of 2
- But there is little excuse for the bad stuff coming up...

14

[2]: Why has PIRA been used?
"If PIRA is so bad why does everyone use it?"

- "Promoted by management consultants and international standards organization" (Hubbard and Evans)
- Subjectivity over probabilities seems to excuse more subjectivity (it doesn't of course!)
- People seem to think it adds value (with little evidence)
- Dropping the maths makes it easier for risk assessors (of course there are better ways of doing that!)
- Avoiding maths might make it seem like we are better at communication and can "see the big picture"
- Laziness?

15

[3] RR examples
HML with contradictory definitions

Table 4.3.1 Consequences - Both Threats and Opportunities

High	Financial impact on the organisation is likely to exceed £x Significant impact on the organisation's strategy or operational activities Significant stakeholder concern
Medium	Financial impact on the organisation likely to be between £x and £y Moderate impact on the organisation's strategy or operational activities Moderate stakeholder concern
Low	Financial impact on the organisation likely to be less that £y Low impact on the organisation's strategy or operational activities Low stakeholder concern

Table 4.3.2 Probability of Occurrence - Threats

Estimation	Description	Indicators
High (Probable)	Likely to occur each year or more than 25% chance of occurrence.	Potential of it occurring several times within the time period (for example - ten years). Has occurred recently.
Medium (Possible)	Likely to occur in a ten year time period or less than 25% chance of occurrence.	Could occur more than once within the time period (for example - ten years). Could be difficult to control due to some external influences. Is there a history of occurrence?
Low (Remote)	Not likely to occur in a ten year period or less than 2% chance of occurrence.	Has not occurred. Unlikely to occur.

- Federation of European Risk Management Associations
- Written in conjunction with AIRMIC, ALARM and IRM

- Some behavioural biases
- Absolute gibberish!
- The more you think about it, the worse it gets

- See (corporate) references for link

[3] RR examples (1)
1-5 in matrix + HML with subjective definitions

Severity / Likelihood	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Frequent					
Probable					
Remote					
Extremely Remote					
Extremely Improbable					

HIGH RISK
MEDIUM RISK
LOW RISK

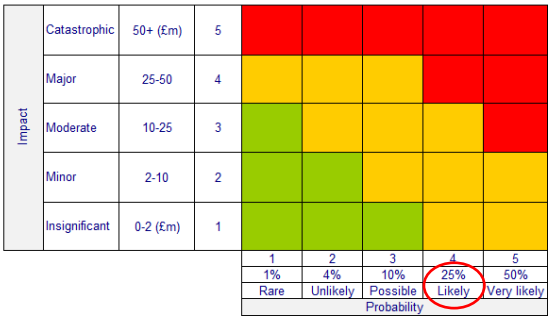
Figure 3 - 1. Predictive Risk Matrix

- US Federal Aviation Administration
- This had better "work"
- Your life in their hands

- Subjective, but comprehensible
- No numbers (yet)

- Page 12 on http://1.usa.gov/OghmEu

[3] RR examples (2)
1-5 with subjective definitions + numbers / ranges



- Unclear ranges for probabilities
- "Likely" = 25%(?) – just shows scope for subjectivity
- Going forward we'll use a tweak to the numbers ...
- ... and drop the description

[3] RR examples (3): PIRA approach
From a distribution to a single number / colour

5	>£100m	5	10	15	20	25	High
4	£50m - £100m	4	8	12	16	20	Medium
3	£10m - £50m	3	6	9	12	15	Low
2	£1m - £10m	2	4	6	8	10	
1	<£1m	1	2	3	4	5	
		<3%	3%-15%	15%-35%	35%-65%	>65%	
		1	2	3	4	5	

- Base P-I table
- We have dropped the labels "major" etc

* >= "weak consistency"
* See maths Appendix

- How might we have got here?
  - Pr(loss>0) and impact distribution
  - Assessor thinks of some event/loss (Best estimate? Disaster in news?)
  - Simplifies this to an impact (say £2m) and a probability (say 20%) (*)
  - **Risk map:** Compresses this to (P,I) = (3,2) – colour amber
  - **Top risks:** Compresses further to 3 * 2 = 6
  - **Actions:** Probably driven by colours or "top risks"

Section 5 gives more on this "downward spiral" of risk assessment

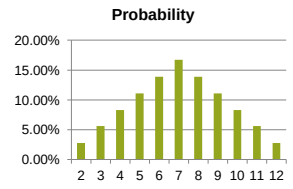
(*) Yes, we know the distribution is continuous – none of it makes sense!

[4] PIRA in theory: dice set-up
(or how to show PIRA is flawed – quickly)

- Two fair dice are rolled
- Pays out £Xm where X is the total score
- [Insurer charges £7.5m (if this affects your risk assessment)]

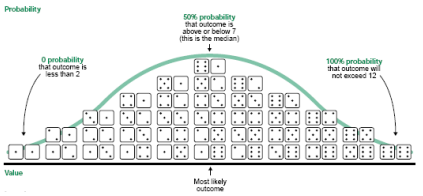
Die 1 ↓		1/36	2/36	3/36	4/36	5/36	6/36 = 16.7%
1	2	3	4	5	6	7	5/36 = 13.9%
2	3	4	5	6	7	8	4/36 = 11.1%
3	4	5	6	7	8	9	3/36 = 8.3%
4	5	6	7	8	9	10	2/36 = 5.6%
5	6	7	8	9	10	11	1/36 = 2.8%
6	7	8	9	10	11	12	
Die 2 →	1	2	3	4	5	6	

[4] PIRA in theory: dice risk
An unfair question?



PAUSE. from the insurer's perspective:

- **What's the risk? [description & number]**
- **What's the probability?**
- **What's the impact?**



n	Prob(n)	Prob(>= n)
2	2.8%	100%
3	5.6%	97.2%
4	8.3%	91.7%
5	11.1%	83.3%
6	13.9%	72.2%
7	16.7%	58.3%
8	13.9%	41.7%
9	11.1%	27.8%
10	8.3%	16.7%
11	5.6%	8.3%
12	2.8%	2.8%

[4] PIRA in theory: dice answers
My expectation of the likely actuarial responses

- Risk description: (see Appendix 6 for some "good" examples)
  - Perhaps: "Paying too much as a result of the dice game"
  - Or perhaps: "The score is more than we assumed in the premium"
- Risk numbers: [the actuary protests]
  - "You haven't given me enough information to put a single number on risk"
  - "It depends what you mean"
- Alternative approaches:
  1. Risk = distribution
  2. Fix impact, deduce probability: the p-value approach
  3. Fix probability, deduce impact: the capital approach

  RRs typically avoid all 3

- Pity the poor "risk owner" (who won't give an actuarial response)
  - Standards give no guidance and don't discuss 1-3
  - So what happens in practice?
  - Who knows what we end up with?!

22

[4] PIRA in theory: dice
"what would PIRA say?"

- Remember the probability-impact matrix?

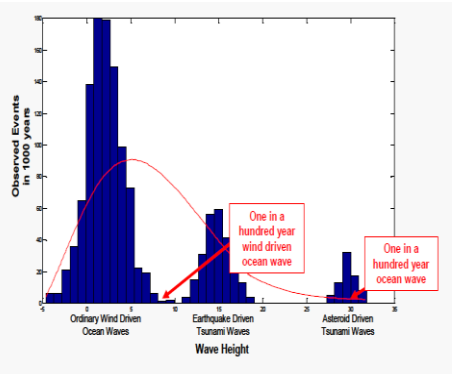
Impact	Single score e.g.	Compound (range) e.g.
1 (< 1m)	N/A; (min is 2)	N/A
2 (1m-10m)	Roll 2 (2.8%) **(P,I) = (1,2)**	Roll 2-10 (91.7%) **(P,I) = (5,2)** Roll 8-10 (33.3%) **(P,I) = (3,2)**
3 (10m-50m)	Roll 11 (5.6%) **(P,I) = (2,3)**	
4 (50m-100m)	N/A; (max is 12)	N/A
5 (> 100m)	N/A	N/A

- All the above probability-impact statements are simultaneously true
- What does the risk register / PIRA approach say?
- **Different people might choose (1,2), (2,3), (5,2) or (3,2)**
- **Without further guidance we have ambiguity and contradictions**

23

[4] PIRA in theory: wave damage
The real world is more complex than dice

- Head office on Florida coast
- What is the risk of wave damage? (weather in general?)
- What are you assessing?
  - "Ordinary" waves?
  - Earthquake-driven?
  - Asteroid-driven?
  - All waves?
- Is this 1 or 3 risks?
- Either way, **impact is a distribution**



- The same "dice" issues remain, hidden by the complexity

[4] PIRA in theory: double subjectivity
Avoidable and unavoidable subjectivity

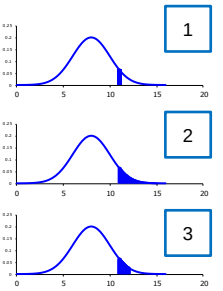
- **Unavoidable:** Real world probabilities are unknown
- Ranges are a poor way to reflect this (if this is their purpose)
- **Avoidable:**
  - Introduced by PIRA methodology i.e. (P,I) indexes ...
  - ... and lack of specification
- Examples of avoidable subjectivity
  - Event or distribution?
  - What part of the distribution (or is that up to the assessor)?
  - What is the point of the ranges? (statistical or parameter?)

- **Let's give that a little more edge**

[4] PIRA in theory: double subjectivity

Avoidable subjectivity: a pictorial summary

- Which of the following are you trying to work out?



1. **A single point (subjective by risk or VaR)**
   Probability p say, point impact 11
2. **A single point (e.g. tVaR approach)**
   Probability (same) p, range impact 11-∞
3. **A range**
   Probability q say, range impact 11-12
4. **A full distribution**
   Probability 1-pr(loss=0), impact 0-∞

- Each of these has different implications for probability and impact
- Uncertainty over impact: → distribution + parameter uncertainty?
- Uncertainty over probability: → distribution
- Is it clear the ranges are not being used to highlight uncertainty?

[5] PIRA in practice

Most PIRA approaches adopt 4-6 below

1. **Risk (impact) distributions (pr(loss>0) + loss distribution)**
2. **Distribution summaries.** e.g. Mean, std dev, percentile
3. **Two-dimensional risk maps.** (P,I) = (0.03, 5m)
4. **Index numbers.** P, I are "looked up" (0.03, 5m) say → (1,2)
5. **Index-based rating.** Rating = product = 1*2 = 2
6. **RAG rating.** One of more of 3-5 above → RAG rating

Assessment (1-3)

Reporting / decisions? (4-6)

This paints a flattering picture of PIRA:

- 1-2 are almost never used (and don't make it through to reporting)
- 3 is usually not explicit i.e. we don't get to see/hear the (0.03, 5m)
- Instead: "I think we need to increase the rating from (2,3) to (2,4)"
- Some suggest that assessors **ignore** the underlying loss ranges

[5] PIRA in practice
A downward spiral: what have we lost? (1)

1. **Move to single numbers rather than distributions so P ε (0,1) and I ε (0,∞) :**
- Assessments are "... quite often chosen to represent some form of defined extreme or 'worst case' scenario" (*)
- We do not know what the risk assessor is targeting
- Different "targets" → risks are almost certainly assessed inconsistently
- Two numbers: statistical and parameter uncertainty has gone (already)

2. **Distribution to (fixed) ranges and look up so P, I ε {1,2,3,4,5}:**
- We've lost whether something is "high" or "low" in the range

3. **Rating = P*I**
- Typically we've lost whether the probability or the impact was high
- These would have had different implications for risk management
- P*I is useless for capital purposes

3. **Colours**
- Yet more scope for inconsistency and confusion

[5] PIRA in practice
A downward spiral: what have we lost? (2)

- Very lossy:
  - We cannot deduce μ, σ, percentile from (P,I)
  - We can't usually deduce (P,I) from P*I (only on the SW/NE diagonal)
  - We cannot recalibrate (say 1-in-20 → 1 in 200)
  - Typical process generates no "audit trail" (assessment, reporting, decision)
- (P,I), P*I or colours are no basis for decisions
- **Methodological "uncertainty suppression" – ironic for risk management**

[5] PIRA in practice: (P, I) assessments
Numerical issues: (1) Different risks, same box

- Problem with using P,I in 1 to 5 (i.e. P-I index)

Risk	Prob	Impact	Best estimate	(P,I)
A	3%	10m	300K	(2,3)
B	15%	50m	7.5m	(2,3)

- In best estimate terms, B = 25*A, but the same box
- **i.e. at best (2,3) is what gets reported**

[5] PIRA in practice: (P, I) assessments
Numerical issues: (2) The wrong way around

- Another problem with using a P-I index

Risk	Prob	Impact	Best estimate	(P,I)
A	66%	10m	6.6m	(5,3)
B	65%	50m	32.5m	(4,3)

- Intuitively we prefer A to B (backed by best estimate)
- PIRA implies A is worse than B
- **At best the (P,I) box is what gets reported**
- P*I and RAG status will also be misleading

- A 5 by 5 (P, I) map is only 33% “mathematically efficient”
- See Appendix 3

[5] PIRA in practice: colours, actions and top risks

Are you confused yet? What about the Board?

- P*I means you can't recover P or I
- And (1,5) is rated the same as (5,1)

5	> £100m	5	10	15	20	25	High
4	£50m - £100m	4	8	12	16	20	Medium
3	£10m - £50m	3	6	9	12	15	Low
2	£1m - £10m	2	4	6	8	10	
1	< £1m	1	2	3	4	5	
		< 3%	3%-15%	15%-35%	35%-65%	> 65%	
		1	2	3	4	5	

- HML = RAG
- 25 and 5 red
- 4 and 10 amber
- (1,5) <> (5,1)

Issues

- **Top risks** are often based on a P*I ranking/rating – but perhaps (x,y)<>(y,x)
- **Risk maps** show (P,I) graph
- **Decisions:** Are we basing actions on (a) colour, (b) P*I or (c) risk appetite?
- These various systems don't fit nicely together

[5] PIRA and colours: a quiz

An unclear basis for action / risk management

5	> £100m	5	10	15	20	25	High
4	£50m - £100m	4	8	12	16	20	Medium
3	£10m - £50m	3	6	9	12	15	Low
2	£1m - £10m	2	4	6	8	10	
1	< £1m	1	2	3	4	5	
		< 3%	3%-15%	15%-35%	35%-65%	> 65%	
		1	2	3	4	5	

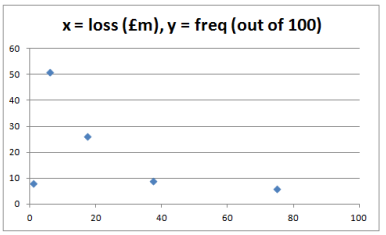
← Reduce?
← Monitor?
← OK?

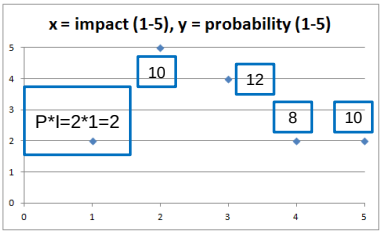
- Assume the colours represent types of required action
- How were the colours set? Were they based on...
  a) the organisation's risk appetite / tolerance?
  b) a cost-benefit approach to risk reduction?
  c) a risk-return approach to risk assumption?
  d) another (unstated) and potentially arbitrary approach?

[5] PIRA and reporting using risk maps
Losing our sense of proportion

- Lognormal simulations of 100 "IID" risks / events

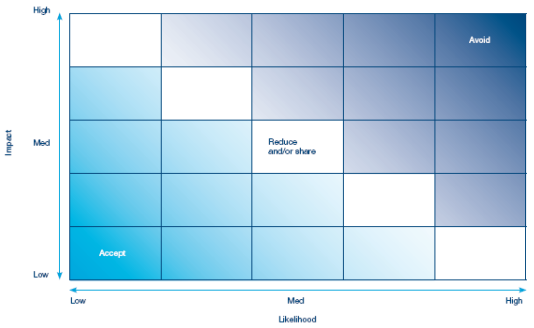
Range (£m)	Loss (£m)	Impact
0-2	1	1
2-10	6	2
10-25	17.5	3
25-50	37.5	4
50+	75	5





- Top: probabilistic presentation
- Bottom: PIRA presentation
- PIRA → expected cost emphasis
- Which is more helpful?
- Actually there's more variation
- [Loss not compressed to average]
- Especially on $(50, \infty)$

[5] PIRA in practice: colours, actions and top risks
People expect this framework to drive actions



- Source: PwC "A practical guide to risk assessment" ... and many others
- On a stand alone basis RRs give no sensible basis for action (Appendix 4)

[5] PIRA in practice: flawed decisions
RRs do not support sensible decision making

- Managing risk by removing the highest scores / colours?
- Instead you want the best total risk reduction for least cost
- Also need to know your budget
- Risk appetite might effectively say
  - "We have no appetite (or competence) for this risk"
  - "Even our assessment might be badly wrong → get rid of it"
- Other risks as part of risk-adjusted value maximisation?
- RRs don't help with much of this

- Conclusion: you'd better be using other tools in order to manage risk
- Again, see Appendix 4 for just a little more on this

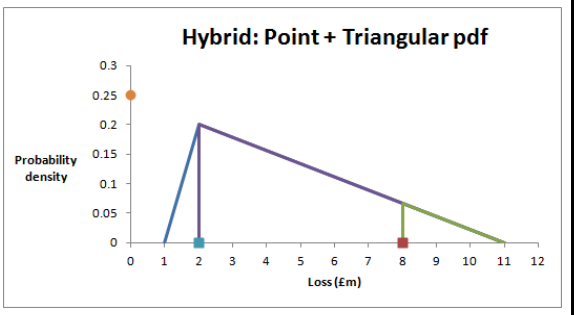
[5] PIRA in practice: flawed decisions
UK scientists give a view

- "The deterministic (aka PIRA) approach requires an evaluation of the likelihood of the impact or losses made from a single specific scenario, quite often chosen to represent some form of defined extreme or 'worst case' scenario. The objective is to represent a range of impacts up to the level of this 'worst case' scenario."
- [As noted, even this is rarely articulated]
- [PIRA-based simulation may be overly prudent for capital calculation]
- "**One key weakness of deterministic assessments is that they are not readily comparable across risks ... comparisons between deterministic scenarios will not be on a consistent basis** as both the likelihood and impact for scenarios will vary."
- **"However in practice, risk managers routinely compare several deterministic scenarios and make decisions on that basis."**
- Source: Blackett review of high impact low probability risks (see references)

[6] Towards better risk assessment: a prototype
1: A hybrid triangular distribution

1. Pr(0 loss) = 0.25
2. Min positive loss = 1
3. Max positive loss = 11
4. Mode = 2

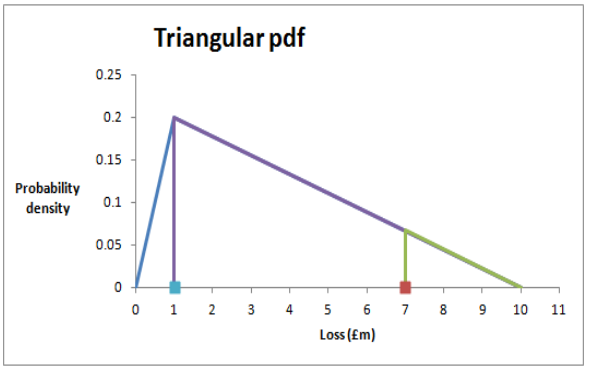
1-4 define the pdf



- Big triangle is the pdf of the loss **given a positive loss**
- The height at "x=2" can be worked out from the
- 1=area (pdf) and area = ½ base * height
- This gives significant flexibility

38

[6] Towards better risk assessment: a prototype
Δ 1: A simplified triangular distribution

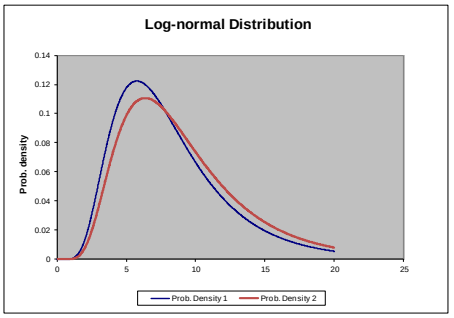


- Max positive loss 10
- Mode = 1
- Hardcode min loss 0

- This distribution is very helpful, **but requires only 2 parameters**
- Mode and maximum: **don't even need to talk about probability!**
- Better communication, though positive pr(loss=0) could be helpful

39

[6] Towards better risk assessment: a prototype
Δ 1: How realistic is a triangular distribution?



- The log-normal is a popular loss distribution
- A triangle distribution with a (min, mode, max) of (1, 2, 17.5) would be a fair fit up to about 15
- If there is no upper bound on losses Δ distribution doesn't really work
- This is only a prototype; can easily be generalised to non-Δ

40

[6] Towards better risk assessment: a prototype
Δ 2: Parameter uncertainty

- In reality we do not know the (mode, max) are (1, 10)
- We could reflect our uncertainty by a second set of Δs
- **Mode:** say (min, mode, max) of (0.5, 1, 1.5)
- **Max:** say (min, mode, max) of (9, 10, 11)

- We're close to being able to do simulations
- See Appendix 5 for a simulation recipe
- Some will simulate (e.g.) for operational risk capital
- *Note that if people are effectively giving a conservative assessment this could lead to conservative capital*
- Need to be clear and explicit

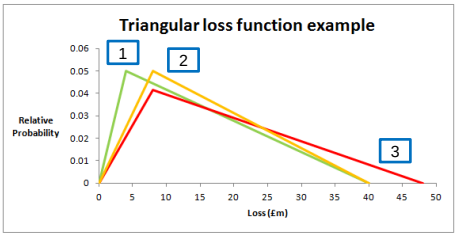
41

[6] Towards better risk assessment: a prototype

How about reporting the mode and a percentile?

Assessment	1		2		3	
	x	y	x	y	x	y
	0	0	0	0	0	0
	4	0.05	8	0.05	8	0.04
	40	0	40	0	48	0

70th percentile impact	28.00	28.69	34.14
Probability (30%?)	3	3	3
Impact (10-50m)	3	3	3



- 3 assessments over time
- Risk owner thinks of Δs!
- Risk owner chooses to assess 70th percentile
- Equate this to 30%
- PIRA says (P,I)=(3,3) for each assessment
- Board will think “no change”
- But in moving from 1 to 3:
  - Best estimate has doubled
  - 70th percentile up by 22%
  - Worst case up by 20%

[7] Even better risk assessment: distributions

Beyond the double Δ prototype

1. Use distributions other than triangles (few new concepts)
2. Use corporate models to quantify impact

   Can we really expect a risk owner to assess the impact of longevity improvements being 1% greater than those priced?
3. Use statistical/economic models to reduce judgement for intermediate results
   - e.g. Vasicek interest rate model for movements (“input impact”)
   - Then the corporate model (as in 2 above) to assess “output impact”

- Time effects: quite straightforward; the mode and max can change over time (see the previous slide)
- Practical point: will the risk owner be willing to change (esp increase) the max over time? – might be better to use the 90th percentile!

[7] Better risk assessment: more models please
Beyond financial models

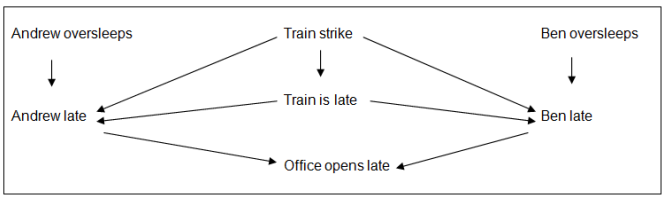
- Traditional financial models may need extending
- Capital models allow for most risks but don't project uncertainty

- Other types of model may be useful for:
  1. Strategic risk
  2. Project risk
  3. ~~Operational~~ Business as usual risk (insurance, credit, liquidity, market, op etc)

- Risk registers often incorporate little of (1) and (2)
- Insurers probably use (some of) the potential models for (1)-(3)
  - but 1 might sit with the business planning team
  - and 2 might sit with the project team
  - That's OK, but are uncertainty management techniques incorporated?

[7] Better risk assessment: dependencies
Operational risk: beyond independence

- Techniques akin to project diagram
- But we ought to understand current processes better than project risks
- Tree diagrams result in probability / risk assessment
- Andrew and Ben are responsible for ensuring the office opens on time.



- Risk: "the office is not open on time"
- The arrow direction indicates causality
- Even this simple diagram shows a process much richer than the usual.
- May be helpful for risk management (probabilities, controls etc)

[7] Better risk assessment: dependencies
No we don't mean correlations...

1. **Dependencies can affect outcomes:**
- **The usual:** gross risks
- **Control-induced:** common controls can increase dependency
2. **Dependencies can affect assessment, hence decisions:**
- Due to common (biased) risk assessment
- This can manifest itself in a large number of ways
3. **Ignoring dependencies can be bad for your (firm's) health**
- Ignoring dependencies in general – Cox (2005) Appendix B
- Substituting correlation for dependency – Ferson Appendix 8

[8] Summary checklist and conclusions
10 ways to get better: there is an alternative

1. Give proper guidance around risk assessment (e.g. %ile)
2. Modify PIRA + ditch fixed ranges and risk = P*I (the worst offender)
3. Think distributions, not events
4. Build a prototype and expand from there
5. Reflect uncertainty over probabilities
6. Use financial models appropriately (e.g. inflation impact)
7. Build mini-models for dependencies (e.g. operational risk)
8. Start building links between RRs and:
   - Capital and other financial models
   - Risk appetite / tolerance (and maybe utility)
9. Less time on 1-in-200 and more on 5%-95% (see Appendix 8)
10. Speak up: expose the emperor's new clothes

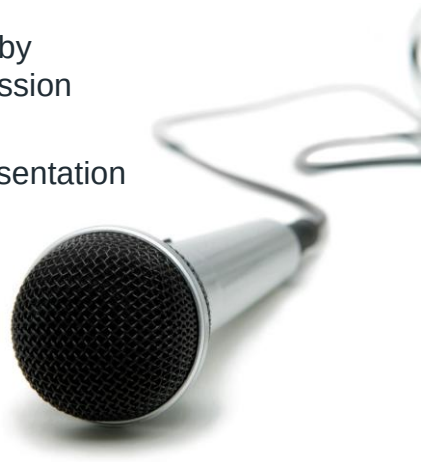
[8] Summary checklist and conclusions
Conclusions ... including some nudity

- The PIRA risk assessment methodology is badly flawed
- Risk registers are (typically) not trustworthy
- There are better alternatives
- Real decisions are (supposedly) being made based on PIRA
- Expose “the Emperor’s new clothes”
- Actuaries should step up and speak up
- Be the boy not the king

Questions or comments?

Expressions of individual views by members of The Actuarial Profession and its staff are encouraged.

The views expressed in this presentation are those of the presenter.



List of Appendices
Those marked * may be of most worth

1. My personal confession
2. * Two risk tools (risk-control matrices and bowtie)
3. The maths of RRs
4. RRs as the basis for risk decisions
5. * Double triangle simulation: a simple recipe
6. Bad features of (typical) RRs
7. * Links and references
8. * Good reads:
   a) Graham: The Great 99.5th Percentile Swindle
   b) Hubbard and Evans: a summary
   c) Ferson et al: a summary of their paper

Appendix 1: A personal confession
Where I'm coming from (aka my bias)

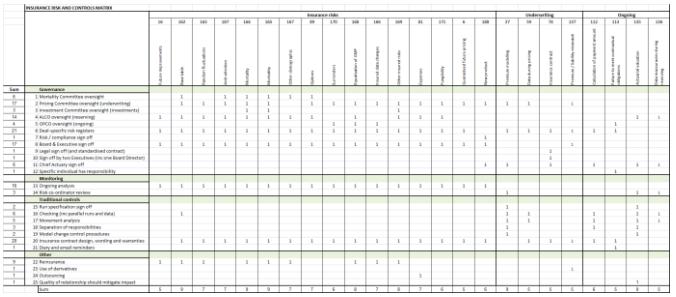
- Risk management suffers from a split personality
  - At times over-quantified: capital at 1-in-200 and way beyond
  - At times under- and mis-quantified: c.f. this presentation
- Neither of these is a robust or scientific (or honest?) approach

1. Graham (GIRO 2011): The great 99.5th percentile swindle
   "Profession should ... issue a statement ... making very clear the inherent impossibility of calculating the 99.5th percentile with confidence"
2. Rebonato: Plight of the Fortune Tellers
3. Hubbard: The Failure of Risk Management
   "... shows how some of the most popular 'risk management' methods are no better than astrology"

Appendix 2: Risk tools - risk-control matrices

Suggested by Leitch, tweaked by Howe

- Risks vs controls (and control type) matrix

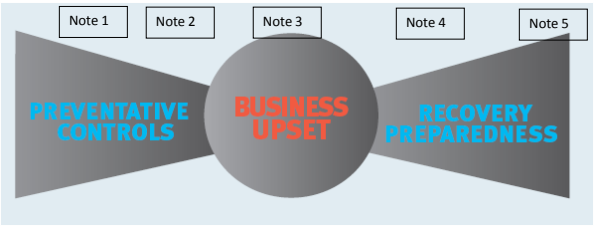


- Risk registers could support risk-control matrices
- But most don't; lots of controls against risks without any overall framework
- Generally an under-emphasis on management / control

- The controls which (are claimed to) apply are easy to review
- Looking down a column shows all the controls applying to a risk (the traditional approach)
- Looking across a row shows all the risks to which a control is applied
- The approach helps us to ask questions such as "why haven't you applied control X to risk Y?"

Appendix 2: Risk tools - the bowtie "timeline"

Some dynamism between risks and controls (etc)



- Diagram source:
- http://bit.ly/Ogxx4K

1. **Controls.** This is where we place controls, i.e. treatments which seek to reduce "the probability".
2. **Risk indicators.** Ideally we have key risk indicators whose role is to place us "on alert". This is easier said than done. For investment risks it could be that risk is reflected in the entry/exit price.
3. **Event (plus).** A "business upset" may be more general (credit loss, economic downturn etc) than an event. Sometimes a discrete event cannot readily be identified.
4. **Mitigations.** These are the things that limit the ultimate impact. The more serious the risk the more mitigations and management action should be planned in advance.
5. **Ultimate impact.** The full outworking of the crystallised risk, potentially with associated corporate and personal regret.

Appendix 3: the maths of RRs

The mathematical efficiency of 5*5 (P,I) maps

- Any two-dimensional comparison is tricky (efficient frontiers)
- We can only strictly compare (P1, I1) and (P2, I2) if ...
- ... (P1 < P2 and I1 < I2) or (P1 > P2 and I1 > I2) *
- A 5 by 5 (P, I) map is only 33% efficient

						Total
5	0	4	8	12	16	40
4	4	6	8	10	12	40
3	8	8	8	8	8	40
2	12	10	8	6	4	40
1	16	12	8	4	0	40
	1	2	3	4	5	200

Rows	5 (R)
Columns	5 (C)
Comparisons	600 RC*(RC-1)
Distinctions	200
Efficiency	33.3%

- * Why can't we strictly compare (1,1) and (1,2)?
- Because of the underlying possibilities...
- ... the risks could be (2%,0.9m) and (1%, 1.5m)
- respectively (1,1) and (1,2)

Appendix 3: the maths of RRs

The mathematical efficiency of general (P,I) maps

R	0	4	8	12	16
...	...	...	...	...	...
...	(R-3)*(C-1)+0	(R-3)*(C-2)+2	(R-3)*(C-3)+4	...	2*(C-1)
2	(R-2)*(C-1)+0	(R-2)*(C-2)+1	(R-2)*(C-3)+2	...	C-1
1	(R-1)*(C-1)	(R-1)*(C-2)	...	(R-1)*1	0
	1	2	...	...	C

Total	Explanation
(R-1)*(C-1)*C/2	
(R-1)*(C-1)*C/2	
(R-1)*(C-1)*C/2	=(R-3)*(C-1)*C/2+2*(C-1)*C/2
(R-1)*(C-1)*C/2	=(R-2)*(C-1)*C/2+(C-1)*C/2
(R-1)*(C-1)*C/2	
R*(R-1)*(C-1)*C/2	

- (R,C) risk map is (R-1)*(C-1) / [2 * (RC-1)] efficient
- The limit as R, C → ∞ is 50%

Efficiency for R,C values from 2 to 10

R / C	2	3	4	5	6	7	9	10
2	16.7%	20.0%	21.4%	22.2%	22.7%	23.1%	23.5%	23.7%
3	20.0%	25.0%	27.3%	28.6%	29.4%	30.0%	30.8%	31.0%
4	21.4%	27.3%	30.0%	31.6%	32.6%	33.3%	34.3%	34.6%
5	22.2%	28.6%	31.6%	33.3%	34.5%	35.3%	36.4%	36.7%
6	22.7%	29.4%	32.6%	34.5%	35.7%	36.6%	37.7%	38.1%
7	23.1%	30.0%	33.3%	35.3%	36.6%	37.5%	38.7%	39.1%
9	23.5%	30.8%	34.3%	36.4%	37.7%	38.7%	40.0%	40.4%
10	23.7%	31.0%	34.6%	36.7%	38.1%	39.1%	40.4%	40.9%

Appendix 3: the maths of RRs
RRs should be "weakly consistent" (at least)

- See "What's wrong with risk matrices?" (Tony Cox)
- "If a decision really matters ..." (red v green, high v low)
- "... then the colours can't share an edge" (or even a corner)
- Arbitrarily small changes in risk can change the decision
- The US FAA isn't even weakly consistent
- You can move from green to red too easily

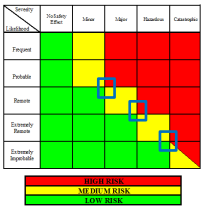
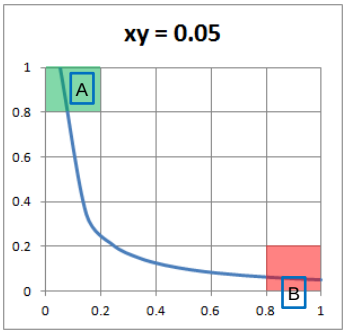


Figure 3 - 1. Predictive Risk Matrix

Appendix 3: the maths of RRs
Another reason for not taking risk = P*I

- Draw an iso-risk curve, along which risk is constant
- If R = P*I this is a rectangular hyperbola
- If R=P*I then actually area A is worse than B, not better



Appendix 4: RRs as the basis for risk decisions
You need more than is in a typical RR

- Risk decisions could be taken based on RR limits or colour
- But the RR contains is insufficient for a sensible decision

- What's over the risk appetite? (rarely the same as RR limits)
- For those which are within the risk appetite:
  - Is there a budget for "risk optimisation"?
  - Can we do a cost-benefit analysis? (just like "non-risk")
  - How about a risk-adjusted financial model?
  - Potentially including risk appetite / utility

- Not doing anything because we're "within limits" makes no sense

Appendix 5: double triangle simulation
A simple recipe*

1. Simulation 1: Rand(0,1) determines mode (via pdf)
2. Sim 2 determines max (ditto)
3. Sim 3 determines loss (pdf is known given 1 and 2)

- Say 1m simulations of 30 risks
- e.g. take 5000th worst gives 1-in-200 result

- As before, take care over dependencies between risks
- * The recipe easily extends:
  - Hybrid- Δ distribution
  - Non- Δ distribution

Appendix 6: Bad features of (typical) RRs
Detail beyond the main presentation (1 of 4)

1. RRs rarely consider total risk
- We have a "portfolio of risks"
- How will this action affect my portfolio risk/return?
- Also shows a lack of integration with capital calculations

2. RR rarely consider dependencies between or within risks
- e.g. Correlation of zero can be consistent with vastly different dependencies and hence risks (see Ferson example in Appendix 8)
- e.g. Different dependencies between drivers of a risk can lead to that risk varying by a factor of 1000+ (see Cox 2005, Appendix B)

Appendix 6: Bad features of (typical) RRs
Detail beyond the main presentation (2 of 4)

3. RRs rarely consider upside risk
- Reinforced by language concentrating on downside rather than uncertainty :
  - "Risk register" not "uncertainty register"
  - "Risk that credit losses are lower than expected" – just sounds odd!
- ✓ Could be described as a "feature" of RRs, not a "bad feature"

4. RRs often display poor integration with the business
- A feature of risk management generally? (despite the hype)
- "Blame apportionment" is not usually attempted
- Poor integration limits the real values of risk management
- "Embedding" back into the business is a poor substitute
- Even risk and capital management can be poorly integrated
- **Paul Klumpes:** "It also seems surprising, given the debate about Solvency II, that there is no explicit link made by the actuarial profession between risk management and capital management. Nowhere is there full discussion of the various links between the two processes and their consequences." http://bit.ly/KXtVol

Appendix 6: Bad features of (typical) RRs
Detail beyond the main presentation (3 of 4)

5. RRs usually make no allowance for known behavioural biases
- The well-documented biases associated with human judgement including that regarding probability and uncertainty
- Often discussed in investment texts
- [This is not the subjectivity often inevitable with even good assessments]
- [This is not the lack of guidance or PIRA's uncertainty compression]
- Hubbard and Evans – page 3
- Kahneman: "Thinking fast and slow"

6. RRs often have poor risk descriptions
- See the next slide for some examples
- c.f. Leitch risk register studies too

Appendix 6: Bad features of (typical) RRs
Detail beyond the main presentation (4 of 4)

ID	Risk	Risk Type	Date opened	Rating (initial)	Rating (current)	Risk level (initial)	Risk level (current)
265	Inability to match resources to demand. Rosters do not match current demand. Weak at weekends.	OPER	31/7/2006	20	20	High	High

Identified risks	Consequence	Action taken to mitigate effects
Reduction in budget: - 1. projected 5% (£25k) 2. projected 10% (£50k) 3. projected 15% (£75k)	Any reduction will impact on provision of services. [Current budget split: - 68.5% - salaries 21.5% - statutory examinations & maintenance of LEVs, & waste disposal. 6.7% - centrally funded services 3.3% - Safety Services running costs]	1. Reduce printing costs, all documents to be web based. Reduce other costs 2. As above & consider increasing existing charges & introducing charges for centrally funded services. 3. As above & consider charging for training

Number	RISK	Rating of significance of risk			Risk owner
		Likelihood	Impact	Overall	
4	Failure to communicate	High	High	High	Head of Communications

- Multiple defns
- In fact statements
- Just confusing
- The irony of it!

Appendix 7: links and references
Previous work on risk matrices / PIRA

1. **Cresswell:** "Qualitative risk assessment and probability impact graphs: time for a reassessment?" Many of the PIRA examples in this presentation were based on the PIRA "matrix" Cresswell supplies http://bit.ly/Mb8q0t
2. **Cox et al (2005):** "Some Limitations of Qualitative Risk Rating Systems" http://bit.ly/Lnx4vL
3. **Cox (2008):** "What's Wrong with Risk Matrices?" http://bit.ly/xHyvhX
4. **Hubbard and Evans (2010):** "Problems with scoring methods and ordinal scales in risk assessment" http://www.dylan.org.uk/ordinal.pdf

- (4) is a particularly strong treatment.
- It omits some of the "paradoxes" of (1) and this presentation...
- ... but covers non-mathematical material given little coverage elsewhere.
- See Appendix 8 for its 4 key points

Appendix 7: links and references
Previous work on risk registers: Matthew Leitch

- Matthew has written a mass of helpful material, including:

1. "Risk register studies"
   - http://www.internalcontrolsdesign.co.uk/rrstudyintro/index.shtml
   - http://www.internalcontrolsdesign.co.uk/rrstudy1
   - http://www.internalcontrolsdesign.co.uk/rrstudy2
2. 2003: "Risk modeling alternatives for risk registers" http://bit.ly/KJ52ve
3. 2003: "Changing risk management to include the upside of risk" http://bit.ly/ModMW3
4. 2004: "What's on your risk registers?" http://bit.ly/LwdJIP
5. 2011: "When is it OK to use a risk register?" http://bit.ly/LM3nTn

Appendix 7: links and references
Corporate stuff

1. **International Actuarial Association** "Guidance paper on ERM for capital adequacy and solvency purposes" http://bit.ly/iNRUsG
2. **"A structured approach to ERM and the requirements of ISO 31000"** http://bit.ly/KCLNU9

   This is a good example of a risk management standard (not necessarily an example of a good risk management standard!) This supplied a "risk process" diagram for this presentation.
3. **Mitre risk process:** http://www.mitre.org/work/sepo/toolkits/risk/StepProcessDiagram.html

   This diagram appeared early on in this presentation and is more detailed than the above
4. **A risk management standard:** http://bit.ly/MTgnUY A good example of woolly verbal labels.
5. **Blackett Review of High Impact Low Probability Risks:** http://bit.ly/IMUmvA

- There is good independent coverage of the value of the PIRA approach in this independent and scientific document. The verdict is damning.
- The report gives three approaches to risk assessment (heuristic, deterministic and probabilistic)
- PIRA is some mix of heuristic and deterministic
- Probabilistic is recommended by the scientists

Appendix 7: links and references
Individuals

- **Sam Savage** got to single triangles before me http://www.stanford.edu/~savage/stat.pdf
- "I am now convinced that modeling every distribution in the world as triangular, specified by a minimum, maximum, and most likely value, would be a significant improvement over the status quo."
- **Kailash Awati** got to double triangles before me http://bit.ly/HfkCui
- **John Norstad** gives an easy introduction to utility (and much more): http://www.norstad.org/finance/
- **Mark Graham:** "The Great 99.5th Percentile Swindle" http://bit.ly/MSvmOJ
- **Scott Ferson et al:** "Dependence in probabilistic modeling..." http://www.ramas.com/depend.zip
- **Shaw et al:** "Measurement and modelling of dependencies in economic capital" http://bit.ly/MYZtV9
- **Embrechts et al:** "Correlation and dependency in risk management: properties and pitfalls" http://bit.ly/KyvCCu
- **Hora:** "Eliciting probabilities from experts" http://bit.ly/MkFe9c
- **Matthew Leitch:** "What's next in the development and use of risk registers?": http://bit.ly/KYKn39 (*)
- **Matthew Leitch:** "Risk management history and regulations (UK)" http://bit.ly/Mwwj0J
- (*) Matthew has a range of original and informative websites including www.workinginuncertainty.co.uk and www.internalcontrolsdesign.co.uk – highly recommended!

Appendix 8: Three recommended reads
Medal winners in an Olympic year

- All the links and references are highly recommended
- e.g. Leitch has a mass of material that will get you thinking widely about risk management in a non-actuarial way!
- But in no particular order:

1. **Graham:** "The Great 99.5th Percentile Swindle"

   The title says it all. Will anyone take up the gauntlet?
2. **Hubbard and Evans:** "Problems with scoring methods and ordinal scales in risk assessment" Wide-ranging coverage.
3. **Ferson et al:** "Dependence in probabilistic modeling..." Superbly written given the relatively technical material on uncertainty and dependence. Striking examples.

- Read on for a summary of 1-3

Appendix 8: Three recommended reads (1)
Graham - The Great 99.5th Percentile Swindle

- Pages 11-13 from Graham's pdf are essential reading e.g.

Actions

What should Companies do?

- As little as possible at the extremes of the distribution as is necessary to get internal model approval.
- Not believe the results from the extremes of the distribution.
- Concentrate on design, parameterisation and use between the [5th] to [95th] percentile, where:
  - Data is more complete
  - History may be a guide
  - Expertise is more relevant
- It is in the central part of the distribution that models can provide valuable insights and, used correctly, add material commercial value.

Appendix 8: Three recommended reads (2)
Hubbard and Evans (H&E)

- Perhaps the best critique of the (mainly) non-mathematical deficiencies of risk registers
- Highlights 4 areas of concern:
  1. Cognitive biases and random variation
  2. Subjectivity of labels (“high”, “very unlikely”, “severe” etc)
  3. Invalid inferences: (1,2) = 2 * (2,1) etc
  4. Invisible correlations
- Suggested “solutions”
  1. Use explicit quantitative probabilities and losses (drop the labels)
  2. Use simulation to model relationships between risks
  3. Correct for biases (e.g. Overconfidence)

Appendix 8: Three recommended reads (2)
Problem 1a - Cognitive biases

- An extensive literature e.g. Tversky and Kahneman
- Wikipedia lists 84 decision-making biases alone (+others)
- H&E: overconfidence, base rate, availability, gambler’s fallacy, optimism, confirmation, anchoring and self-serving.
- Here are two particularly relevant to risk assessment

1. **Overconfidence:** “90% of cases lie between A and B”. Research H&E refer to suggests 55%-78% not 90%
2. **Availability:** “Has occurred recently”. c.f. Risk management standard(!) example in this presentation

Appendix 8: Three recommended reads (2)
Problem 1b: Random variation (or inconsistency)

- Presented with the same data would experts agree?
- Would a given expert give the same opinion a few days later?
- In 1968 x-ray specialists were shown cases a week apart
- Just 0.6 correlation between prognoses

Appendix 8: Three recommended reads (2)
Problem 1: Making allowance

- Allowance for biases and variation can be made:
  - Public surveys
  - Personality-type questionnaires (e.g. interview process)
  - Visual field test (i.e. eyesight)

Appendix 8: Three recommended reads (2)
Problems 2 and 3

- **2: Verbal labels**
- Yet another reason we might get inconsistency!
- "Severe" simply means different things to different people

- **3: Invalid inferences (linear scale interpretation)**
- An impact of 2 is not (usually) twice the impact of 1 (etc)
- "A certain kind of mental discipline and mathematical sophistication is needed to remember that one is using an ordinal scale... We suspect this is often lacking..."
- Even more from those receiving reports (AH)
- And even more when looking at P*I (AH)

Appendix 8: Three recommended reads (2)
Problem 4: invisible correlation

- That's *certainly* the case with risk registers
- Modelling some form of dependence would be good
- There follows a non-Wikipedia example...
- ... Which shows that even zero correlation can be complex

Appendix 8: Three recommended reads (3)
Ferson et al: how hard can zero correlation be?

- Of course we often *mean* zero dependency not correlation
- Same thing for jointly normal variables...
- ... but be very careful
- Take discrete random variables X and Y
- Assume both a distributed uniformly on {1,2,3, ... ,24, 25}
- You are given that corr(X,Y) = 0
- This does not imply independence (of course!)
- Questions: what are the possibilities for

1. min(X+Y)?
2. Prob(X+Y=14)?

Appendix 8: Three recommended reads (3)
Ferson et al: how hard can zero correlation be?

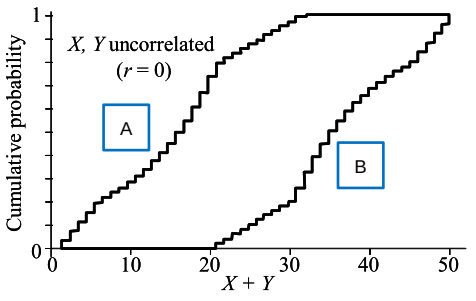


Figure 9: Bounds on the distribution of the sum $X+Y$ given that X and Y are uncorrelated and identically distributed as discrete uniforms on [1,25].

- Ferson et al paper
- Sobering isn't it?
- Each marginal is discrete u(1,25)
- Corr(X,Y) = 0
- **CDF of X+Y could be A or B!**

1. **min(X+Y):** from 2 to 21
2. **prob(X+Y=14):** from 0 to 0.4