### Intro

Hello. I'm Andy Garlick and I have a website called cloudsofvagueness.com which I’m trying to use to improve the way organisations do risk management. As part of this I've recently been looking at risk management standards such as ISO 31000 and what I'm trying to do in this presentation is give an idea as to how they could be improved.

I guess the purpose of a standard is to help organisations establish good practice. I think the problem with doing this for risk management is that good practice has yet to be established, or rather that there is a range of practices that are good and what’s more some are more suited to one organisations that another. And beyond this, there are some areas where there is a dearth of any practice that could be regarded as good.

The water is further muddied by a wide variety of accepted practices and common practices - good or not - and, of course the silly cliché of ‘best practice’, so beloved of the political classes, in Britain at least.

ISO 31000 - and the others - pretend this is not the case. As a result they are cluttered with all kinds of stuff which may be OK in some circumstances, but not others, and it’s hard to get a sense of perspective. The result is often some mixture of motherhood and vague hints which seems devoid of any concrete meaning. This is exacerbated by a generally sloppy approach to defined terms and drafting. They are often imprecise, unrigorous, illogical, inconsistent and so on.

So this is my attempt to do better with a pretend standard!

What I’m proposing is a very stripped down, minimalist approach which will give us better opportunities to reflect the range of current practices and potential future possibilities in a more useful way. It was originally based on ISO 31000 but has come some way since. What I've tried to do is to cut out unnecessary features, use more exact definitions and create a very short set of principles - the body of the standard - which give us the opportunity to understand the concepts better. This also sets the stage for expanding on the potential range of practices in other presentations.

You’ll have noticed that this talk is in the form of a Prezi - rather a dull one - with an audio commentary. Apart from amusing myself during the quiet summer with new technology I have tried to make sure that what is on the screen is the ‘what’ of the standard. And this is intended to be comprehensive. The soundtrack is supposed to cover the ‘why’: why it is what it is and why it’s not something else. All the way through I’ve give some pointers to other material on clouds of vagueness. Indeed this presentation is based on two posts called Pendant’s Corner, 1 and 2, though things have changed a bit in the compilation.

What I’ll do is first of all set out some defined terms, and then come to the principles which comprise the substance of the standard. I’ll give a brief overview of the contents of the supporting guidance documents - these are hypothetical for the time being - and finish off with a quick review of the 11 principles of ISO 31000 to make sure we’ve picked up on them.

So let’s leap to the definitions, starting with risk itself.

### Risk

So we've got something very simple here, the possibility of more than one future: we can’t be certain what’s going to happen. We could replace the definition with uncertainty about the future but I've decided to stick with the r-word for the time being just for a bit of continuity and to avoid confusion with other uncertainty concepts. A presentation called uncertainty governance would sound a bit odd!

Unlike 31000 which talks about the effect of uncertainty on objectives we don't mention objectives at all. This will all come out in the wash when we come to characterising our risk, that is, thinking about the possibilities the future may hold. As far as the definition goes it’s just an unnecessary complication but in fact driving your risk thinking off your objectives can be quite bad practice. Quite simply, it restricts your thinking and what’s more it doesn’t recognise the possibility of adapting to changing circumstances including changing your objectives.

There's also no idea of deviating from the expected future as per 31000. Again this is unnecessary to making progress. This neatly avoids all the problems with defining what an expected future is, an issue sidestepped by 31000.

And obviously there's no idea of upside or downside. I won't be talking about opportunity in this presentation. The concepts are quite confused and we're much better off without any of all that. I'll be coming back to it in subsequent ones or, for a bit of a hint, you can read the cloudsofvagueness post called ‘Always look on the bright side of life’.

Finally it’s worth saying, though it should be obvious, that with this definition risk is going to cover all types of risk, from safety to strategic to black swans.

Now we’ve defined risk we can come to the subject of our standard.

### Risk Governance

Maybe we can’t be certain what’s going to happen but we certainly *can* work to promote futures we like the look of over futures we don’t like to the look of. This is the essence of risk management, or as I prefer to call it here, risk governance.

I've not used the term risk management because it’s actually quite difficult to differentiate it from management *per se*. If you're talking about promoting the realisation of preferred possible futures then that's what management itself is about. Presumably we don’t employ managers to change the past or to make things worse in the future, though sometimes you wonder on both counts! We’ll be talking about the relationship between risk management and everything-else management in more detail shortly.

Instead we're focussing on the governance concept: the idea that thinking about risk, the possibility of more than one future, is an important and serious part of organisational governance. I think this sets the right tone and presages some serious thought and activity. Risk governance will be deliberate, comprehensive and visible. It is much preferable to the rather bland risk management term.

We’ll have a few defined terms for what we should do as part of risk governance, but first let’s just make the obvious step and come to the final top level definition.

### Risk Performance

Yes, we all know it! You can’t manage what you don’t measure.

So we come to risk performance, the extent to which preferred futures materialise compared with less preferred futures. It’s will provide a measure of the success of risk governance. So it’s obviously important, key to the whole idea of risk management, but we need to do quite a lot more work to put some meat on this. How are we going to identify and define preferred futures - presumably this is where our objectives will come in - as well as the less preferred ones?

How will we implement slightly woolly concepts like ‘the extent to which’?

In fact this uncovers the point that risk performance is not a particularly well understood area of risk management and we're going to have to think about it quite a lot more when we come to looking in detail.

### Risk Attitude

Now were' going to look at some of the definitions which are key to thinking about the ingredients of risk governance, starting with risk attitude.

Obviously it's important that the organisation worries about what risks it faces and what it's going to do about them, so this is the starting point. An alternative term for this might be risk policy. In fact both are defined terms in 31000. This one is more or less verbatim, though I’ve dropped something about assessment which I think is unnecessary, while policy is about a statement and covers all of risk management. Again these additional aspects should come out in the wash, as we’ll see.

### Risk Controls

Next we have risk controls - actions which are expected to improve risk performance and promote better futures. Obviously we don't look at actions which are not expected to improve risk performance!

This is a slight tweaking of the 31000 concept which is about modifying risk. My approach puts more emphasis on the risk performance concept which is essentially missing from 31000. In any case, so far we have introduced risk only as the concept of different possible futures, not as something that has a measured level to be modified. Of course we’ll have to tackle this eventually, but not as part of the high level discussion.

It's important to recognise that this definition covers both routine controls - corporate anti-fraud procedures, for example - and one-off controls - maybe an additional concrete quality test, or patenting an invention. The distinction doesn't matter for our purposes, at least for the time being.

What we are also saying is that the controls may either be options for consideration previous to decisions or selected actions which have been agreed to be put in place as part of the decision process. We’ll come back to the decision process in more detail shortly.

### Risk Analysis

Next we have risk analysis, the process to characterise risk. The purpose of this will be to inform decisions so it’s worth being clear that risk analysis needs to characterise risk under all the options for action - the risk controls - under consideration.

I‘ve adapted the term slightly from 31000 in such a way that it should explicitly cover risk identification and determining the level of risk.

At this stage we don't need to separate out risk identification. Risk identification may not even be appropriate and it is here that 31000 slips into talking about individual ‘risks’ with no definition of what it’s talking about - how the concept differs from ‘risk’ - the effect of uncertainty on objectives.

We also don't mention the level of risk yet. We haven’t introduced the tools for this yet and we don’t need to at this, er, level. We’ll pick up on this when we look at the whole question of risk analysis in a lot more detail later in supporting guidance documents. Since risk analysis is my speciality there is already quite a lot on clouds of vagueness - as well as more to come!

### Risk Evaluation

Next we come to risk evaluation, the process of comparing the options for action in the light of the results of the risk analysis and the organisation's risk attitude. So it creates the idea of putting the characterisation of risk side by side with the risk attitude.

In fact we might want to rejig the definition to something like ‘consider the results of the risk analysis in the light of the organisation’s risk attitude’.

This is clearly part of decision making and is a seductively simple idea but one that is overegged. In general you need to look at other factors as well in a decision. Sometimes you can just say a risk is intolerable - a bit of safety risk speak which is overdone in the general risk context- but being able to reach a decision on the basis of the risk evaluation alone should be the exception not the rule.

(next slide)

As a result I'm not actually convinced that we need this definition; we could just feed the results of the risk analysis and the risk attitude into the overall decision process. This would simply the slide a bit.

But what we have done here is dispense with the idea of the ‘risk criterion’ one of the most egregious of the 31000 concepts. This is discussed further in several clouds of vagueness articles on risk appetite.

### Risk Behaviour

For our final definition we come to risk behaviour, the risk related activities (or even inactivity) by individuals, groups or the organisation at all levels.

So it relates to recognising risk, making decisions about what to do as result and doing it. It applies to all risks, and unlike the risk attitude which is an organisational concept, this applies to individuals as well. You can see that this going to lead into the risk culture idea but I thought it best to stick with behaviour as that's something that’s observable, at least in principle.

The official definition of risk culture, at least according to the IRM begins, “the values, beliefs, knowledge and understanding about risk shared by a group of people ....” This is clearly more difficult to pin down than actual behaviour.

### Principle 1

With these 8 definitions we can now start to write down the first element of our standard, Principle 1. And this just describes what the organisation should do about risk governance. This has got three essential elements.

First of all it's important that the organisation defines its risk attitude, what risk - possible futures - it faces, what it wants to do about this risk and so on.

Secondly it needs to focus on having the right organisational characteristics so that the risk behaviour will ensure the provisions of its risk attitude are realised. Remember risk attitude is about the organisation as whole, whilst risk behaviour and achieving suitable risk behaviour is about the individuals and groups at all levels and all roles in the organisation and covers how they deal with all categories of risks.

The role of risk behaviour in risk governance can be formal or informal whether it’s to do with how we identify risk, how we feel about risk and how we act on risk. We have to recognise that a lot of risk governance is completely informal, determined by people’s risk awareness and behaviour and passes under the radar of the more formal processes.

This brings us to the third point which is taking account of risk in decisions. Of course decisions can be formal or informal but we're particularly thinking here of the role of risk evaluation, a rather formal process which is based, as we said, on the risk attitude and the risk analysis and the available risk controls.

A risk evaluation has to be factored into all decisions, either formally or informally, at all levels in the organisation. But decisions are not totally about risk. Some are, for example safety decisions as part of safety management often happen in their own corner and don't need to consider other disciplines. By contrast, while strategic decisions obviously have to take risk on board, they're not all about risk. Risk is just one thing to be considered and the risk evaluation comes in alongside the economic evaluation, the social evaluation and so on.

This emphasises a very important point that risk management, risk governance, is not an isolated set of activities and processes. Perhaps the biggest criticism which is made of the risk management practices which have been employed up to now is that they tend to be standalone - add-ons which don't get integrated into the organisation as a whole. What's important to recognise is that that shouldn't be the case and that it doesn’t make sense, for example, to talk about risk decisions. So that last part of Principle 1 is all about integration. We'll look at that in a bit more detail now.

### Management

Our route to this is to consider a generic management loop of the plan-do-review type. Within an organisation the situation is a lot more complicated up and down, within silos and so on. But what I want to do here is systematically discuss the risk aspect of each element of the loop.

This typical management loop could apply to the management of anything. Let’s trigger the loop by starting with the options. Some of the options would include options for risk controls. These are then evaluated and the evaluation takes on board the risk evaluation. As I mentioned this combines the risk analysis of the options and also the risk attitude. Based on the evaluation of the options you make a decision. So you need to be able to take risk on board in your decision processes.

Hopefully you implement what you have decided. I'm not going to put a lot of emphasis on doing what you say you're going to do but it's a common feature of risk governance, especially if it is not embedded, that often the actions, the risk controls that you've decided to implement, are not in fact carried out.

And then we reach the back half of the cycle where we talk about monitoring and review and these both have very important risk aspects as well. Monitoring leads us to our second principle and review will lead us to our third principle as we'll see.

It’s worth saying that I had some difficulty in deciding what aspects of risk governance should be regarded as integrated into ‘everything else’ management and which needed its own risk-relevant definition and principle. It’s a bit arbitrary and I based my approach to some extent on whether there is anything risk-specific to say. In the end I felt that no decision should in principle be a risk decision in isolation, though I did keep risk evaluation. I also kept risk controls although they could have been just part of the general actions planned or implemented.

But back to our principles.

### Principle 2

These last two points of the management cycle lead us to our final two principles - everything we need to complete our standard.

The second principle is that organisations should monitor their risk performance and act on the results. ‘Monitor’ has its own technical definition (not specifically risk-related) which I've included on the slide. Essentially, the idea is that you look to see how you're doing, looking at performance indicators and focussing on risk as well as other things. So this is another key integration point. Essentially some of the indicators on your balanced scorecard should relate to risk.

The key question raised is: what is ‘required or expected’? Evidently organisations will need to define triggers for actions as well as the indicators themselves.

Once your monitoring shows that you have identified a change from the performance level required or expected the action that is triggered is to go back into the plan-do-review management cycle and decide whether you need to have a different set of risk controls as well as potentially other actions to change performance levels that come out. As far as risk goes, you're looking to change the risk controls either in the light of the performance or maybe in the light of new risks emerging: a significant change in the profile of possible futures.

I recognise this is quite conceptual at this stage. As I’ve already mentioned risk performance measurement is not so well developed and I’ll come back to the realities of this when I talk about guidance in this area.

### Principle 3

And now the final principle - organisations should visibly review their risk governance and act on the results.

Again review is a technical/quality-type term and I've included the definition on the slide. The purpose of the review is to determine the suitability, adequacy and effectiveness of the subject matter, in this case risk governance, and again I’ve included 'act on the results' so that risk governance is indeed suitable, adequate and effective.

I've also said that the organisation should *visibly* review their risk governance. I think this is a key element of risk governance. Risk management can be in place informally but the formal part of risk governance ensures that there is some ability for stakeholders to see what it is that's going on. This aligns with the tone set by the use of the word governance that I mentioned earlier.

Thus stakeholders can see the processes that are being employed - risk analysis maybe, the culture improvement programme or whatever it is - but also the content, the specific risk issues, the specific risk controls, to make sure the items are there which people think should be there. Or, indeed if other risk issues should be recognised, or other risk controls then that can be taken on board as well.

This principle contains the real meat of the standard. In spite of its brevity, following though all the facets of risk management which have been covered would provide a comprehensive and extensive menu for risk governance review. This standard has aimed to achieve this without pointless repetition.

### Next Steps

So that completes our picture of the risk standard and it also provides some really useful pointers as to what sort of guidance we might want to produce to scope out the specific practices which organisations might want to consider for their risk governance. I can see 5 documents.

#### Risk attitude definition

First of all how to define your risk attitude. I think this can replace quite a lot of nonsensical stuff about risk appetite as I’ve itemised on clouds of vagueness. We need to make sure that this is only concerned with the organisation; it is not directly related to individual risk attitudes. The guidance will need to cover all sorts of risk and the Kaplan and Mikes categorisation is helpful here (see the clouds of vagueness post called ‘we need to talk’).

We will also need to recognise a spectrum of risk attitudes such as compliance or intolerable, prudential or as low as reasonably practical, risk benefit ratios and - most importantly - risk reward. The idea that you have to take risk to be in business but you don’t take more than you have to.

There's a lot work to do to develop a standard approach to defining risk attitude and I think framing it in this way will help us to see what the task is.

#### Risk behaviour improvement

The next one, improving risk behaviours, is intended to cover the risk culture ground. One good sourcebook is the IRM report with the ABC model: attitude, behaviour, culture. As I explained before I've focussed on B rather than C (and A here is more about individual attitudes rather than the organisational attitude of the last point). It's important to recognise that behaviour and culture need to cover the individual, group and the organisational levels.

More important guidance comes through from work in safety culture, covering risk awareness or risk blindness, openness and honesty, doing what you said you'd do an so on. One specific objective is to inculcate mindfulness into the organisation as discussed in clouds of vagueness under resilience (part 2).

#### Risk analysis and decisions

Risk analysis, much more interesting to me, and since I’m in advertising mode you can read my book. We need to be clear that risk registers, risk lists, are not the only way to characterise the range of potential futures and are not necessarily the best. And again, negative risks are not necessarily the way to deal with upside and opportunity. Of course we then have to approach the question of what's better and there there's a lot of work to do.

It is here that the ISO 31000 material on setting the context will appear. I think this is a little over-egged, but it’s nonetheless good practice to understand the context and nature of something that is being risk analysed and risk managed.

We haven't really mentioned levels of risk yet, but our guidance here will need to, with an extended discussion of subjective probability. It will also cover the semi-quantitative stuff (with some stark warnings) and maybe a plea for quantification a la Hubbard (see my clouds of vagueness post called ‘proud to be a war quant’).

Perhaps the most important point is not to overinflate our expectations of risk analysis. Characterising the range of possible futures with some estimates of the likelihood of each is a ridiculously ambitious objective. (See the clouds of vagueness commentaries on Naseem Nicholas Taleb’s books.) My conclusion from this is that we need to switch to a greater focus on risk culture in the way that I’ve already described. This goes some way to explaining why it is covered in this standard but not ISO 31000.

#### Risk performance monitoring

Risk performance monitoring - another interesting area which I’ve already mentioned as being underexplored. Key risk indicators - KRIs - and associated triggers are quite well developed in the financial area (and sometimes confused with risk appetite) and we need to do more work on them to see how we can develop the idea for other environments and how it fits into a general KPI, balanced scorecard environment.

And one area I’ve glossed over with regard to risk performance monitoring is the need to monitor the environment to see what’s changing. If a risk decision process is to be triggered by risk performance monitoring anomalies, then this needs to include the emergence of new risks or other aspects of the external environment.

#### Risk governance review

Finally risk governance review. What we do here should be obvious going back to the definitions of the various components of risk governance and here we have got a fairly good guide as to what reviewing risk governance and acting on the results of the review will give us. The guidance will just need to plod though all of this making sure everything is covered, including setting up the risk governance arrangements in the first place.

I haven’t said much about stakeholders and communication. It is for each organisation to decide what is to be made visible as part of the review and to whom. In fact I have tacitly assumed that when information about risk governance is communicated through the visibility requirement then this is part of the review. If it’s not for review, why are you doing it? It’s possible this is one simplifying step too far.

### ISO 31000

In comparison with the existing standard I have made several fundamental changes - but as I ought to acknowledge, kept lots of stuff. This work builds on 31000.

First I have stripped down the terminology. Definitions which do not appear here include: risk management policy, risk management plan, risk owner, establishing the context et al, communications and consultation, stakeholder, risk assessment, risk identification, and many other specialist risk analysis terms including likelihood, risk profile, risk criteria, risk treatment and residual risk. In contrast 31000 does not mention risk behaviour/culture.

Second, I have not bothered with risk framework (which I don’t properly understand - that is, I think it’s not properly thought through or described) and risk process.

Finally I have not been driven by the 11 principles which are supposed to be requirements for effective risk management. I thought it would be worth checking how they are dealt with in my scheme.

* Risk management creates and protects value - presumably a statement of better futures compared with worse.
* Risk management is an Integral part of all organisational processes - this is overblown but covered by the integration discussion.
* Risk management is part of decision making - Principle 1.
* Risk management explicitly addresses uncertainty - er, yes, obviously, given risk equals uncertainty.
* Risk management is systematic, structured and timely - presumably the review would reveal any failure on these scores.
* Risk management is based on best available information - I’m starting to lose the will to live.
* Risk management is tailored - yes, but this is not discussed helpfully by 31000.
* Risk management takes human and cultural factors into account - but not as much as here.
* Risk management is transparent and inclusive - transparent means you can’t see and I’ve no idea what inclusive means here. In fact it’s just appropriate communication and involvement which is being got at.
* Risk management is dynamic, iterative and responsive to change -well we’ve got our three cycles.
* Risk management facilitates continual improvement - this somewhat grandiose explanation is not actually reflected in the detail which is about the improvement which will come from review.

In short these principles are really just fluffy aspirational statement of what will emerge from good risk governance. They don’t drive it.

### Summary

So there's our risk standard, set alongside ISO 31000. We've got the 8 definitions; we've got the relationship, the integration, with normal management processes; we've got our three principles which actually form the standard; and we've got a clear roadmap for the next steps in terms of future guidance documents. In these we will be able to record current practices, explore possible future practices and so on in a framework which has been set up to support exactly this.

I think some interesting trends have emerged. We need to think more about risk performance and its role as part of performance management. We need to think more about risk culture. We need to shift our thinking from risk appetite to risk attitude. (Or, more accurately, we should ditch the risk appetite term.) We probably need to worry less about risk analysis, though it would be good to have some fresh perspectives on this.

This framework has been kept brief. It is not difficult conceptually. It’s not final: there is still plenty of scope to fiddle around with the basic idea. And its’ only fair to say that I’ve used this exercise to espouse my own manifesto for risk management improvement.

Nonetheless, when the meat has been put on these bones we will have quite volume of material documenting good risk governance practice. Which is what we need.