

Why internal audit fails and what it should learn from Rumsfield's Law of Uncertainty

This is a paper in our 'Internal Audit Futures' series, viewpoints on the evolution of internal auditing.

Many internal auditors feel they are in a losing race against destiny. A great auditor may identify and report on 99 out of every 100 serious threats to the business, but eventually something will get through and the question will be asked "how did audit miss that?" Usually when that happens there are a lot of other people in the organisation to blame as well, but that doesn't detract from the fact that internal audit exists to identify and report on threats and to justify its existence it really needs to be very good indeed at doing that. But 99 successes in 100 is not good enough if that one failure is as destructive as much of the fallout of the credit crunch has been. And being realistic, most audit teams aren't shooting 99%. Raising internal audit's threat detection capability needs a new approach to the way internal audit plan and deliver their work. Enter Donald Rumsfield and his Law of Uncertainty:

"... there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know."

"there are known knowns"

This is the comfort zone, where the vast majority of internal audit effort is focused. The risks are familiar ones and audit knows with a lot of confidence where they need to do work to provide assurance on them. The core of almost every audit plan is based on this view of the hotspots, one where familiar risks are mapped onto familiar business processes – knowns mapped against knowns. The quality of these plans varies somewhat depending on the completeness of audit's views on risk



and process, but this misses the point that these views are fundamentally poor at capturing the threat of the unknown and unexpected. Internal audit needs to accept reality - we are just not good enough at assessing risks for this method to ever be comprehensive and accurate. No one is good enough, it can't be done, the world (and any one business) is just too complex for us to rely on audit plans made up of the known knowns. One response to fast moving risks is to run a flexible audit plan linked to a frequently updated risk assessment, but this doesn't greatly improve assurance as it doesn't overcome the inherent fallibility of human risk assessments.

This is not an argument for junking these risk assessments. The risks they identify are 'core' to the organisation and they need to be assured. They are also the natural subject of an internal audit opinion – assurance that defined risks in defined parts of the business are adequately managed. The argument here is that audit needs to spend less time on these risks through

a combination of more efficient systematic approaches (routine audits on routine risks) and overall increased productivity (making every audit function as efficient as the best 20% would double productivity for most functions). Time saved would then be used to tackle the other categories of Rumsfield's Law.

“there are known unknowns”

For internal audit to do a better job, it needs to change the balance of its efforts and build real agility into its working methods. The known unknowns are one of the areas it needs to respond to. These are issues in the business which are known, to the extent that some problem is recognised, but the real extent of the threat is not understood, by internal audit and usually not by management. The reason for focusing audit effort on these issues is the very evident reality that most major issues that damage an organisation don't appear entirely without warning signs. In many years of investigating major control failures there is almost always some smaller issue, of falling standards, apparently minor errors, or just concern voiced within the business, which was ignored as unimportant or low priority and which preceded the blow-up. Internal audit needs to react to these warning signs with rapid, precise (and small) exploratory reviews to identify root cause of the issues and the potential for severe problems. These reviews dramatically increase the likelihood that audit will be ahead of the blow-up and have the chance to flag the threat. They also fit well with the kind of skills internal audit typically has on staff. The major challenges are:

- being networked well enough in the business to hear about the issues when they happen;
- judging when you have enough information to reach a conclusion on the threat, and then walk away - getting bogged down in insignificant issues which are a major waste of time and expending time to generate action plans on issues without major risk potential will cripple your resourcing, unless the business is happy for you to resource up for that effort;



- having audit staff who are comfortable jumping into issues with little preparation time, able to multi-task between an issue review and a core audit, or many issue reviews, and savvy enough to see the bigger implications of a small event. Auditors with real operational experience are a big help in making the judgements these reviews require.

These exploratory reviews need only generate limited audit documentation, focused on the issue and its causes and potential risks. Short form reports in memorandum style add to the efficiency of the exercise.

“there are also unknown unknowns”

Black Swan theory is much in vogue of late. It is an attractive theory as it deflects much personal blame – “it was a black swan event, no one could have seen it coming.” It is also in danger of being overused. Few events actually meet the criteria that ‘no one’ saw it coming. Internal audit can be so much more valuable to their organisation if they are the ones who ‘saw it coming’ by identifying the threat early. In response to black swan theory we have entitled our daily blog Black Turkey Event, dedicated in part to risks that are foreseeable but might be missed or ignored. For instance liquidity risk, or call it cash funding risk, was not on many audit agendas in late 2007, or through much of the first half of 2008. Can we really argue that was a black swan? Certainly not after the failure of Northern Rock in September 2007, and there were warning signs before that. And at the time of writing (March 2009) how many audit agendas include the risk of significantly increased inflation levels? There are a mountain of warning signs of that emerging risk going back well into last year.

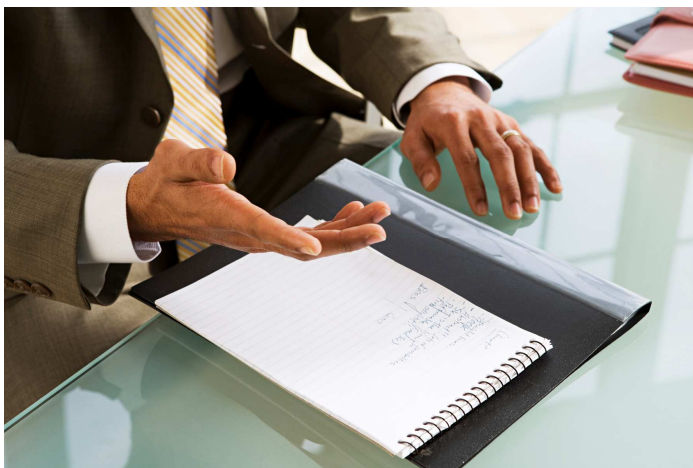
To address these unknown unknowns, the threats that no one is really certain of, internal audit need to become very good at something many functions have long talked about – scanning the horizon for threats (emerging trends in the economy, bad news from other organisations, regulatory or legal strawmen, concerns of contrarian thinkers) and acting early on them, assessing whether they could ‘happen here’ and how bad might it be. To do this well takes dedicated time, leaving it to auditors during their day job will not and has not worked. It requires time spent on reading widely and monitoring events – the great virtue of the internet age is that there are immense quantities of information and viewpoints, insights and analysis on which to draw. Once you know where the best sources are they are easy to tap into and track. This is not a blank cheque on resource, a half an FTE equates to a great deal of threat scanning and communication of those threats.

Time is then needed to investigate the potential of these threats to damage your organisation. A rapid initial assessment will usually determine whether more work is needed. Engaging the right people to make this assessment is key, technical specialists and external

experts might both be involved. In either case internal audit needs to be in control of the analysis, questioning judgements based on little evidence and playing the role of devil's advocate to management complacency.

Once a plausible threat is confirmed internal audit needs to be prepared to kick off detailed reviews, major pieces of work in some cases, to assess how vulnerable their business is to that threat. These reviews are where this approach can generate a major resource impact, and for that to work audit needs a workplan which is flexible enough to adapt to a large additional review being added usually at short notice.

Do threat scanning well, treat it as a core activity done by your best people and act on the plausible threats they identify, and internal audit will have closed off one of its great blindspots.



In larger organisations risk management functions may lay claim to do the things described here, and in some cases they might. If that is something you can audit and place the highest level of reliance upon then that is the right thing to do. But realise how important these activities are and place the bar for assurance equally high.

And will it always work?

No. But tackling methodically and with energy all three elements of Rumsfield's Law will produce dramatically better results than the overwhelming focus of today on the known knowns. As an approach it needs to be explained to the Executive and Audit Committee - the only obstacle there may be that this is what they think they are already getting. It needs to be reflected in resourcing plans, a much smaller time allocated to fixed 'core' audits (with the efficiency challenge that comes with that) and significant chunks of time set aside for reviewing emerging issues within the business and threats that are highlighted from events outside. Finally, reporting to the Audit Committee needs to be adapted to reflect the results of these different elements of work. But the outcome is worth the effort of change - the business will be better protected and internal audit will be a more agile and exciting place to work.

Kingston Smith Consulting LLP, the business protection consultancy, is ideally placed to help internal audit review their effectiveness and develop the tools and approaches they need to succeed in the most demanding of environments.

About Kingston Smith Consulting LLP

Kingston Smith Consulting is the specialist consulting practice associated with the top 20 accountancy firm Kingston Smith LLP.

Kingston Smith was originally formed in 1923 and the firm has grown to its current position through organic growth and mergers. Kingston Smith is a member of KS International which is an association of independent accounting firms in over 50 countries around the world.

Kingston Smith Consulting LLP

Devonshire House, 60 Goswell Road, London EC1M 7AD, UK Telephone +44 (0)20 7566 4000 Fax +44 (0)20 7566 4010 info@kscllp.co.uk www.kscllp.co.uk

A list of partners is available for inspection at the above address.

Registered in England and Wales as a Limited Liability Partnership: No OC341786 Registered office: Devonshire House, 60 Goswell Road, London EC1M 7AD