WORKING WITH OTHER ASSURANCE PROVIDERS

In this latest article on audit basics, Bev Cole explores the an area that has developed beyond recognition in the last ten years or so, and that is working with other assurance providers. Bev is an independent consultant on Internal Audit and Risk Management and is Chair of the ACCA's Member Network Panel on Internal Audit.

Welcome to the last article in the back to basics series, which covers how best to work with other assurance providers. No doubt we will be revisiting earlier topics in future newsletters. In this article I will be exploring four aspects of the topic: who the other assurance providers are likely to be; what information we should consider sharing and why; what reliance Internal Audit can place on their work and how; and finally the emerging area of integrated assurance reporting.

Firstly though, I will just briefly cover why this is becoming such an important topic for large organisations. When I first worked in a bank in 1988, there was no Compliance function and no Operational Risk function. Internal Audit was itself undertaking compliance checks as a result of the recently introduced Financial Services Act. There was no robustly defined risk appetite, no risk registers, no key risk indicators and limited incident reporting. Now a large bank will employ hundreds and hundreds of people in their 2nd line of defence. The explosion in information on risk is almost overwhelming. The fact that this has coincided with the near collapse of the Financial Services industry is a topic for another article, but it does make you think!

Internal Audit cannot ignore these functions and the plethora of information available. It cannot go about audits as it used to ten or twenty years ago. If it does, then it will not be serving its organisation well and it will create duplication of effort and additional cost. Not least, it will annoy management intensely, as they get sick to death of what they perceive as an 'army of checkers' constantly on their backs. In addition, it will not use information which could provide valuable insights into the assessments it is performing. For the purposes of this article, I will assume you are working in a large organisation, as this is most likely to have a number of assurance providers and may well operate using the three lines of defence model (the first line being line management, the second providing risk oversight, and the third being Internal Audit).

Other Assurance Providers – Who Are They?

Some of the assurance providers are comparatively new, and some always existed, but we didn't think of them as being risk owners or providing elements of risk oversight. The most important ones are sitting in your 2nd line of defence and include your Risk Department; Compliance Department and your Sarbanes-Oxley Team if you have a US listing. Your Risk Department is likely to include sections bespoke to the risks you face in your industry. For example, in a bank it will include credit, liquidity, market and operational risk. In other industries other risks will be key, for example in Oil and Gas

your Health and Safety team will be very important. In manufacturing organisations, your Quality teams will be important.

In addition, your Operational Risk Team will co-ordinate across teams within the business who have risk oversight of a specific risk category, for example IT Risk or Fraud Risk. The operational risk management framework will almost certainly require the following to be in place across these risk categories: risk appetite (often in the form of Key Risk Indicators (KRIs)); risk registers (containing key risks and mitigating controls); incident reporting; loss reporting; and monthly risk reporting to the Operational Risk Committee. In addition they *may* require these teams to verify that the key controls mitigating the material risks across the Group are operating correctly. These checks are likely to include a sample of business areas only and be undertaken periodically.

The 2nd line may well assess and place reliance on the checks undertaken by line management who, as the 1st line of defence, will also be providing assurance. This view is more likely to be focussed on Key Performance Indicators (KPIs), although some have KRIs too. Line management are likely to undertake quality assessments on the work of their teams, often involving control compliance checks and exception reporting from their IT systems. Line management's checks are likely to be frequent and undertaken as a routine aspect of supervision. For controls / rules which are material to the organisation as a whole, line management may have a breach reporting process. For example, in banks, the Treasury department will report breaches as a matter of course. Other incident reporting processes can include IT incidents, security incidents and business continuity incidents. Please note that there may be duplication between incident / breach reporting in the first line and incident reporting through operational risk, although you may find more detailed information is collected in the first line.

There are external sources of assurance as well. These are likely to provide useful information for assurance planning, but should not be relied on by Internal Audit within their audits as the work undertaken is, by definition, not part of the management and control framework within the organisation. External sources of assurance include External Audit Management Letters; and reports from your Regulators / tax inspectors. In addition, management may well commission assurance work externally, for example from the Big 4 consultancy businesses. These are often used where a view is needed on industry good practice, a highly technical issue, or emerging regulation.

At this point I thought it would be useful to remind you of the key attributes of Internal Audit's work. Firstly it is *independent* and *objective* and therefore is a very strong form of assurance as it is unbiased. Secondly it is *reasonable* assurance, so it is sample based and does not cover all activities or departments. Thirdly it forms part of the *governance* of an organisation and not its management, therefore the checks we undertake are less frequent than those of the 1st or 2nd lines of defence.

In a large organisation, robust management of risk and the governance of it requires all three lines of defence to be in place, but it also requires these three 'cogs' to work as designed in order for the machine to work correctly. If the 2nd line places reliance on the 3rd, the 1st leaves the control checks to the 2nd, the 2nd undertakes oversight as if it's the 3rd, the 3rd doesn't assess the assurance provided by the 1st or 2nd, then the likely outcome is chaos and a weakening of control. This potentially could have disastrous consequences; it is vital that each line of defence understands its role and that of the others and sticks to it.

Information Sharing – what and why?

Information sharing is two way and I'll start with Internal Audit receiving information. In the context of working with other assurance providers, then we are interested in information to assess the risk and control environments. Some information will be useful for your assurance planning; some for your assignment planning; some for your assignment fieldwork and some to provide context for either your assignment or assurance reporting.

From the 1st line of defence, you may find the following useful: risk registers; breach reports; monthly management committee packs; KPIs; KRIs if available at a departmental level; exception reports; quality reports; SOX documentation and testing results; and independent consultants' reports.

From the 2nd line of defence, the following may prove useful: risk appetite and KRIs; monthly risk reports by risk category; incidents reported; Committee packs such as from the Operational Risk Committee; risk registers by risk category; SOX reports; 2nd line inspection / compliance reports; and independent consultants' reports. I have put incident reports in the 2nd line as it is easier and more reliable to request that they are automatically forwarded to you by your Operational Risk team.

Your external sources of information include External Audit's management letter; reports following visits by your Regulator or the tax authorities; and reports on 3rd parties – i.e. SAS 70 reports [now SSAE 16 in the US and ISAE 3402 internationally] (from an in depth external audit of a service organisation's control objectives and activities), evidence of compliance with quality standards etc.

Turning it around, what are the other assurance functions likely to want in terms of information from you? The depth of information and format obviously depends on the area in question, but broadly they want to know your audit plan; audit report ratings; material issues raised and if they are being addressed effectively; and material issues accepted. In my opinion, in a large organisation where you have a lot of audit data, you can add value by sharing this information wisely.

Obviously you need controls around the sharing of audit information, for example, to whom you are able to send a copy of the audit report and whose permission do you

need? I think it is best to agree this at an overarching level generally. For example, you could agree with your Audit Committee that the audit plan and audit reports can be sent to your Regulator and to External Audit if requested and I would also expect your Risk Department to automatically receive a copy of the audit plan and reports.

Below this level it can get 'political' over what information is shared. One way I have used in the past to get around this is to 'tag' individual findings to a risk category on your audit database. Then reports of all issues linked to, for example fraud risk, can be sent in a monthly report to the risk oversight area, in this case Fraud Risk Management. This bypasses the sending of entire audit reports including executive summaries and opinions, although it is not without problem as issues can often be linked to two risk categories using either cause or effect. For example, an issue may lead to fraud (Fraud Risk), but be caused by staff not complying with controls and this not being picked up by supervision (HR risk).

Please, please, please do not forget that this only represents the sharing of written information. Often the best information sharing is verbal. Having a good relationship with senior management within the other assurance functions is vital. It's much better to hear of an emerging issue in a phone call, than wait up to six weeks for it to appear in a report!

One word of warning, you *must* put in place an efficient process for handling this information otherwise you *will* get overloaded. The last thing you want is for all of your auditors to spend half their time reading incidents and committee packs. You may wish to have a knowledge management policy in place which, as a minimum, maps the information available and where it is kept within the Department. And don't forget to have a document retention policy in place and to keep the often confidential information securely, only for as long as you need it, and restricted to those who need to know. The approach I have taken in the past is to have one of my team as lead for a business area or risk category. They can spend up to a day a month reading and analysing relevant information and summarising key highlights for those in the team that need to know, and then briefing them.

The other action you can take to keep informed is to attend management committee or risk committee meetings which receive and discuss assurance. Another word of warning here, if you do attend regularly then you MUST ensure that the terms of reference of the committee have you as an attendee and not a member, and that you have no voting rights. One of the risks of this approach is that the committee turns to you on matters relating to risk management or control, rather than looking to management. It MUST be clear that you are an observer, although that does not prevent you raising issues where others round the table don't.

Placing Reliance on Other Assurance Work

Often this is seen as a tricky area. In a drive to cut cost or to avoid perceived duplication, there is a risk that some Audit Departments place total reliance on the work of the 2nd line of defence, without even assessing it. Anecdotally I have heard that some even go as far as avoiding that subject if there has been some risk oversight of it. Others I have heard of go the complete other way and audit as if the other assurance doesn't exist and ignore a potentially very strong control. In my view the correct answer, as is often the case, is somewhere in the middle.

A good way to think of other assurance is just as any other control over the management of risk. Like all the other controls, you need to assess it in terms of its design, then test compliance with the control and then test substantively to see whether the control has been effective in managing the risk. Only at that point, can you then look at how this control changes your perception of the risk and of the controls that you as Internal Audit need to test. Obviously in the case of other assurance, the 'control' in question will itself be comprised of a number of different controls.

So to take one example, say you are looking to audit reconciliations and you find that Finance has a team performing a 2nd line of defence role for reconciliations across the business. They set the policy; design the process for submitting reconciliations to Finance; monitor the timeliness of returns; monitor reconciling differences and challenge where necessary; and have periodic inspections over compliance with policy and controls within business teams. Within the audit you would look at the design of the policy and process, and you would look at the control to ensure all reconciliations required were received on time and reconciling differences were monitored and challenged. Then before looking at individual business reconciliations, you would assess how effective the reconciliations inspection team is. This would include: how they selected departments to visit; frequency of coverage; what their inspection program looked at (including substantive testing); the quality of their reports; and whether action was taken as a result. In addition you would both compliance and substantively test a small sample of the reconciliations they inspected to ensure you would draw the same conclusions. Further testing would depend on the outcome of this assessment.

As can be seen in the example above, whether you can avoid duplication or not depends largely on the assessment of the 2nd line controls, although some duplication is inevitable in order for you to test the effectiveness of the 2nd line controls. What you should remember when challenged over perceived duplication is that your assessment alone is independent and objective and that it is only undertaken periodically. So for example in the scenario above, it may be in Finance's short term interests to falsely report the number of inspection visits undertaken or to say they are challenging reconciling differences where they are not. Conversely, where Finance's controls are strong it must be remembered that their controls are operating monthly, with

inspections undertaken on a sample of areas probably every quarter, with data on reconciliations likely to be reported monthly, whereas your audit may only be undertaken every couple of years.

One word of warning is that the same 2nd line control can appear in lots of different audits. The most efficient and effective approach is to design your coverage to avoid re-confirming and testing them each time. This is logical and obvious when written in an article such as this, but the practicalities are not so easy. Business auditors should be encouraged to approach the auditors of the 2nd lines initially rather than approach them directly. These auditors should know the controls in place, when they were last audited and the results. If you do not do this, then you could end up with dozens of individual auditors contacting one team, such as Operational Risk, with the same query. Similarly when auditing the controls in a 2nd line of defence area, if you find material weaknesses then ensure that the business audit teams this may impact are also aware. Finally, remember when planning your audits to work with the other assurance functions over timing of visits to the business to minimise the perceived 'army of checkers' problem.

Integrated Assurance Reporting

This is a new area which is still developing. It has arisen from concerns from the Board / Audit Committee that the information they are receiving from the various assurance functions is contradictory. They would often like to see one organisation wide version of the truth on risk and control, presented in one report.

My personal view is that there is great value in presenting the views of the various assurance functions in one report, a form of assurance mapping and reporting. However, I do not believe that the report should endeavour to present 'one true view', rather that is should present the different views together with an explanation of why they are different. To me, to do otherwise would be to destroy the very strength generated by having three lines of defence with different but aligned jobs to do.

I also believe that wanting a single view is a symptom of the lack of understanding at times by management of these different roles. This often manifests in other complaints such as there being an 'army of checkers' or duplication by Audit, Risk and Compliance. Therefore in my opinion one of the opportunities being presented by integrated assurance reporting is the opportunity to get across how the various forms of assurance differ and what their strengths and weaknesses are.

To illustrate this I have included below a table demonstrating some of the assurance attributes by assurance provider. This is based on my experience, and the reality will vary from company to company. The High / Med / Low ratings given show *relatively* how the areas compare, and do not represent an absolute measure.

Robustness* - factors I have taken into account on robustness include independence and objectivity; professional standards and approach; professional qualifications; quality

control; robust sample selection and sizing etc. Therefore, for example, SOX cannot be rated as High as the central team will set the process and controls themselves and therefore will not be completely independent or objective. Similarly 1st Line Management's assurance is shown as low as it is self-assessed.

Assurance Provider	*Robustness**	*Business Coverage*	*Depth*	*Frequency of checks*	*Scope*
Internal Audit	High	Sample of areas	Med	Low	All risks
Operational Risk	Medium	All areas	Med /Low	Med /Low	Op risks
Compliance	Medium	Sample of areas	Med / High	Med	Regulatory risk
Business Continuity	Medium	Majority of areas	Med	Med	Business continuity risk
SOX	Medium	All material areas	Med**	Med	Financial reporting
1st line of defence	Low	Business dept only	High	High	All risks for dept

** only scored as medium due to the very high materiality figures often used, Internal Audit would be looking at a lower materiality in my experience.

As you can see from the table above, in my opinion the robustness of assurance gets higher as you move outwards from the 1st line, to the 2nd, then to the 3rd. Conversely the frequency of 'checks' goes the other way, with Internal Audit being the least frequent and management checks the most frequent.

The aspect the table cannot bring out effectively is the different perspectives as driven by the different remits and objectives of the various lines of defence. 1st line management will supervise staff and do quality control checks on the aspects most important to their own goals, such as customer sales, customer service and processing accuracy. 2nd lines focussing on a particular risk category such as Compliance on Regulatory risk, will obviously focus a lot of attention on controls over a few narrow aspects, for example, compliance with regulated sales rules and controls. They themselves may place some reliance within their work on 1st line management's supervisory controls. Operational Risk will challenge business areas' risk registers, but a lot of their reporting is metrics-based using Key Risk Indicators. Internal Audit will probably pick a mix of perspectives to audit and cover risk categories, departments and processes. Our reporting is based on our opinion over the effectiveness of controls to manage risk based on robust evidence, and should provide this opinion against the context of the stated risk appetite.

As you can see above, it is very easy to misunderstand the exact scope and coverage of assurance provided and how robust it really is. Perspectives and opinions on how well risk is being managed may vary just because of these factors. For example, management's checks on a topic may be more recent, but not as robust as Internal Audit's. Conversely, in sampling business areas and transactions to provide *reasonable* assurance, Internal Audit may well have missed a 'hot spot' appearing in other assurance reporting. And Operation Risk may pick up deteriorating KRIs which control assessments wouldn't necessarily have predicted. To me the power is in presenting all views and explaining the differences, or undertaking further investigations if necessary into the differences.

So, what could an integrated assurance report look like? It does lend itself to visual representation and one option would be a grid with risk categories down one side and assurance areas across the other, and 'traffic light' opinions where they intersect. To me a lot of the power, however, is in the analysis and explanation of the differences. Remember, the differences may all present a true picture, but based on looking at slightly different things or at different times. For example, it would be good to see and understand what is going on when, for example, line management's quality control checks shows that control is working (Green), Operation Risk KRIs show risk metrics have deteriorated (Red), and Internal Audit said in a report a few months previously that control design needs to be improved (Amber). This could very easily represent a true view, i.e. that weaknesses in the design of control are impacting how effectively risk is being managed, but that staff are complying with the controls as designed.

As your integrated assurance reporting develops, you could produce more granular information, breaking down risk categories into specific key risks (sub-risks) and also looking at assurance over the operation of key controls.

Why should we move towards integrated reporting? I have already described some of the drivers, such as the Board's request for one version of the truth due to the differing views they see. Other drivers include the huge amount of risk information now being presented; increasing risk contagion; the increasing complexity of risk management in certain industries; increasing regulation; the maturing of risk management; and the drive for efficiency and cost savings.

What does this mean for Internal Audit? It's a bit too early to say, but in my opinion it could be a huge opportunity for us to re-establish our position at the forefront of providing assurance. For example, Internal Audit could drive the integrated assurance reporting process and drive out and understand those differences mentioned above. We *should* drive it if we perceive it to be part of governance and therefore in need of independent and objective explanation.

We could also use it to define what assurance is and to explain and educate on the differences in roles of the various assurance functions. It would aid our view of

assurance governance and we could highlight actual gaps and overlaps within it. We could use it to sell the benefits of Internal Audit and reiterate our position as providing the most robust assurance due to our independence and objectivity, together with our professional standards, qualifications and rigorous, evidence based approach. We could also explain what the other assurance areas provide that we don't.

And what if we don't take this opportunity? Well, there will probably be increasing pressure for cost cutting and a reduction in often incorrectly perceived duplication of work by Internal Audit. Ultimately we risk a weakening of our voice on assurance and potentially a 'false' assurance picture being unwittingly presented to the Board, with potentially disastrous consequences.

So, my view is that we should take up the challenge, show our initiative and lead from the front on integrated assurance reporting. It will also assist us in building better working relationships with the other assurance providers and should lead to an improvement in information sharing and an improved understanding of where we can place reliance on their work. All of which shows that we are working efficiently, effectively and in the best interests of the organisation.