Gaps and overlaps

Integrating assurance across the business

We need more assurance! It's a natural reaction in response to bad news or in the face of uncertainty. And indeed, there could be some critical areas where you don't have enough assurance. On the other hand, there may also be areas where you feel you are over-assured for the risk involved.

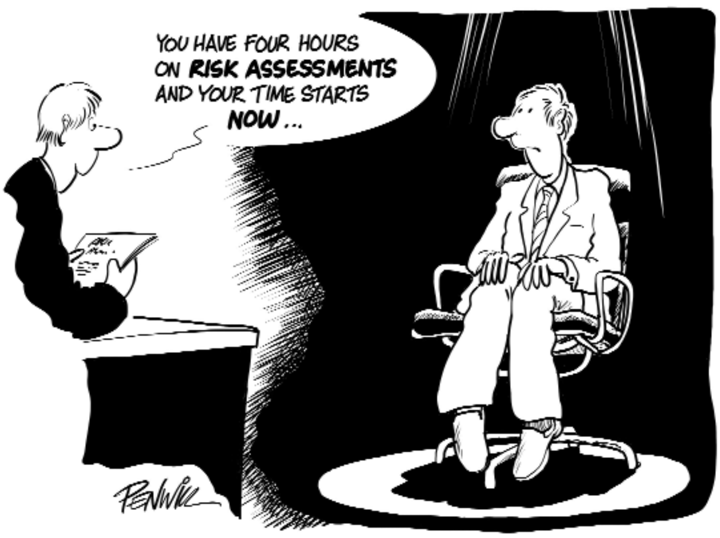
Meanwhile, behind the scenes sits the "assurance cottage industry". If you're not careful, risk management processes and getting assurance can end up being a costly and burdensome distraction to the day-to-day running of the business. Cost, distraction, gaps and overlaps – if any of these symptoms sound familiar, then you are probably asking yourself "How serious is the problem? And what can I do to fix it?"

The growing challenge

Starting at the top of the organisation, the board is seeking to fulfil its oversight role, both directly and through its committees. It's the job of non-executive directors to challenge. They ask lots of questions – at least the good ones do – and they expect answers in return.

And, quite reasonably, directors are concerned about their personal liability. The demand for assurance is likely to increase, not decrease.

In response to this demand, there are typically multiple sources of assurance in any organisation. Internal audit provides objective assurance, to the board and its audit committee, over key financial controls and possibly over wider operational controls. External audit provides independent assurance, to shareholders and to the board, on the financial statements. If you have separate risk and compliance functions, they too are a source of assurance. And health and safety, project office, business continuity, legal, and other specialist functions all chip in.



This isn't an assurance factory so much as an entire industrial estate. And at the same time, management are conducting their own assessments of risk and executive directors are giving formal attestations on the system of internal control. Then, should another Sarbanes-Oxley type initiative come along, a new assurance project kicks off. In spite of all of this, there may still be assurance gaps, but it is hard to tell from looking at the separate pieces of the jigsaw puzzle.

As a result, the assurance operating model is becoming progressively more challenging and complex, with each regulatory change introducing another set of demands. As each initiative translates into business as usual, it leaves behind a legacy of cost and infrastructure that often is not well integrated with other assurance activities. Every silo has its own functional owner, but no one seems to own the whole assurance operating model or have the mandate to make it leaner and smarter.

Beware the risk of too many risk assessments!

Have you ever counted the number of risk assessments made about your business? Different risk assessments could be compiled by risk management, internal audit, external audit, regulators, departmental management, country and product heads, compliance, health & safety, environmental, ethical standards, business continuity, strategic planners and legal, to name but a few…

An inconsistent or misaligned approach introduces its own risks. How well aligned are your risk assessments? Is anything missing? Does "top down" integrate with "bottom up"? How much effort is expended comparing and collating different risk assessments? Can your organisation manage to bring these together effectively, without creating a risk register that is excessive in length?

The size of the prize

Many organisations do not know their total cost of assurance. In determining the total, internal costs associated with risk, compliance and internal audit – at least – all need to be taken into account. When some of these costs are decentralised or combined with other operational activities, things can get tricky, although not impossible.

Add to this the cost of external audit and expenditure on other external accreditation. Then, the total also needs to capture the management time that goes into providing regular assurance reports, plus the inconvenience of additional reporting if something goes wrong.

But even without a precise measure, one thing is clear – it's a big number.

Cost comes in many guises

Quite apart from the obvious cash costs, is your business bearing any of these burdens?

- overly complex governance and control structures
- assurance and control fatigue in the business, as a result of uncoordinated inspection visits and in response to burgeoning regulatory changes
- increasing direct costs of assurance and compliance, at a time when the rest of the organisation is striving to reduce its cost base and improve efficiency
- overlapping risk assessments and control assertions, using inconsistent terminology, data and approaches, all of which cause confusion in the business
- inefficient use of people and technology to support assurance processes and reporting.

An integrated approach to assurance can bring substantial cost benefits. In our experience, a saving of 20% to 30% of the total cost of assurance is a realistic target for many organisations. And that doesn't include the benefit that the business gets from working with a simpler, more aligned assurance framework.

The cost savings are tempting. But the effectiveness angle is equally important, and should carry substantial weight in the eyes of the Audit Committee.

Not many boards or audit committees are presented with an integrated assurance picture. Instead, they are left piecing together different messages, having separate conversations and trying to form a coherent view from disparate sources. This makes it difficult for them to understand or appreciate the actual extent of the assurance coverage, never mind the results.

Integrated assurance gives them much more confidence in the effectiveness of their oversight.

Improved effectiveness

A major financial institution embarked on a risk and control convergence project. Knowing the challenges of assessing the potential cost reductions, but convinced of the wider benefits, they initially took it on faith that the cost benefits would follow. They got started by working on ways to achieve:

- greater clarity on who is delivering assurance, and what is being delivered
- better alignment between assurance delivery and what is actually needed
- less confusion and inconsistency in the information presented to give assurance
- reduced disruption and distraction on the day-to-day business management
- more effective use of time, looking at issues rather than turning the handle on a process
- a better foundation for responding to further regulatory changes.

As the project progressed, the emerging benefits were quantified into a formal business case which confirmed that the project was well worth continuing. In the meantime, they had already started seeing good results and had begun to create momentum for the bigger changes to follow.

Adopting the right attitude

Different parts of an organisation are managed and measured separately. Audit committees also tend to take a silo view because that is how the reporting lines work. If an organisation is going to develop a more integrated approach to assurance and achieve risk and control convergence, it has to overcome inbuilt attitudes, beliefs and structures that support the status quo.

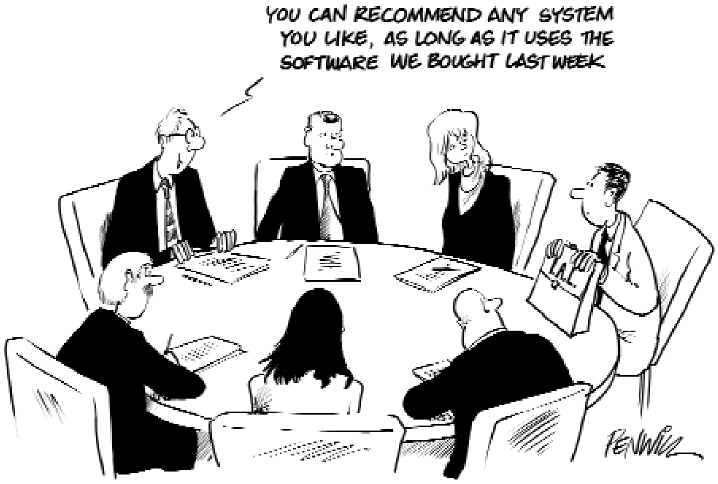
Imagine you could start with a blank sheet of paper. When taking a fresh look at how it all fits together, be prepared to leave behind the baggage. It is only natural to try to hold onto legacy assurance mechanisms, and for each silo owner to adopt a "not invented here" mentality. The right answer might be "best in breed", drawing on practices already in place, but there has to be a willingness to take on fresh ideas as well.

Take a holistic view. The "three lines of defence" model is a great concept, but it can encourage silo mentality. When you strip it down to its component parts of data, processes and systems, and then look at new ways to put it back together again, a number of opportunities emerge for sharing information, people, automation and processes. Assurance needs to be working well as an integrated whole, not just an inefficient aggregation of individually effective parts.

Put everything in the pot. It is also tempting to leave some elements of the operating model untouched, because they are too political or difficult to tackle. Resist the temptation. Every time part of the framework is excluded, the potential benefits case is reduced. Initially, everything should be fair game. Sacred cows might end up with protection, but that decision should be made in the light of the cost/benefit analysis, not by excluding them from the analysis in the first place. Even projects in mid-flight should be considered; otherwise you will finish rationalisation only to find another part added.

Mind the gaps. You have probably been asked the "what keeps you awake at night?" question. An assurance map helps to identify overlaps, but it also helps to pick out the gaps where assurance isn't being provided by the current structures and processes.

When dealing with so many vested interests, you will almost certainly find it helpful to have input from someone independent, to challenge entrenched thinking and to arbitrate on the tough decisions. That can itself present a problem, if it causes the whole thing to feel like yet another "big consulting project", with the injustice of paying consultants to rationalise initiatives they implemented in the first place.



This is an understandable reaction, but not a very helpful one. Better to manage consultants wisely, and scope their involvement so as to get high-value independent advice without it leading to lots of chargeable hours on implementation.

Some practical examples

Putting integrated assurance in place requires a high degree of collaboration and a willingness to share common solutions. For example:

- reporting to the Audit Committee that combines information from various assurance sources
- one issues-tracking system, jointly used for all audit, compliance and Sarbanes-Oxley issues
- integrating "top down" and "bottom up" risk assessments from the business with project risk assessments and risk scenarios
- consistent terminology in the categorisation of risk exposures and control weaknesses
- using one risk assessment to drive risk-based plans for internal audit, compliance and business continuity planning
- a single software solution to support the needs of risk management, Sarbanes-Oxley and internal audit
- joint inspection visits by compliance monitoring, fraud prevention and internal audit
- using the same operational loss data for risk-based capital calculations, forensic investigation and negotiation of insurance cover.

Getting started

The best approach will vary, depending on the organisation and the extent to which it will need to inject independence and objectivity from an external catalyst. But here are some recurring themes.

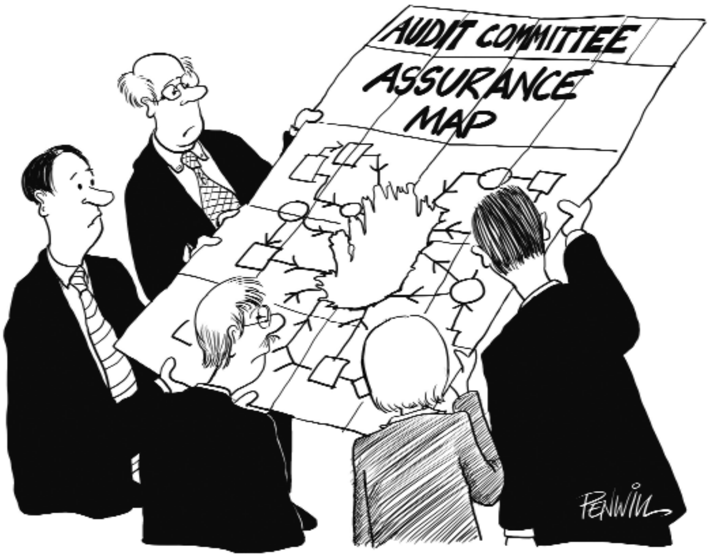
Understand the assurance objectives. There are typically a number of stakeholders involved, all with different ideas on what assurance is required. It makes sense to start with an understanding of needs, current and future, then refine it and prioritise it. Each of these needs will require differing degrees of independence and technical expertise in order for the assurance to be robust. The needs assessment and assurance mapping should look across all the different types of risk, but avoid compiling a wish list of assurance that would be "nice to have". As with overhead cost analysis, you can take a "zero-based" approach to assurance and gradually build up a picture of what is actually needed. A helpful principle is to focus on the purpose behind the assurance.

Challenge the effectiveness, then the efficiency. If you start with an analysis of assurance needs by stakeholder, rather than the assurance delivery by providers, you will usually get a more streamlined set of requirements. It is also a good way to open a debate on effectiveness, before moving on to compare the costs against the assurance priorities. At a high level, the analysis needs to draw out both overlaps and gaps. At a detailed level, it needs to pick out opportunities to share delivery components. And don't get fooled into complacency by benchmarking data that merely confirms you are just as bad as everyone else…

Analyse the costs and the delivery. Until there is a cost identified with providing a particular assurance output, it's hard to win the argument on how much value is released by rationalising it. Compiling an assurance inventory and conducting the cost analysis is not a trivial exercise, especially when you include all of the implicit costs, but it usually needs to be done. Sometimes there is data from costing reviews or re-engineering projects to give a head start, but it is also important to identify the infrastructure costs (data, processes, systems, reports, etc). Remember to include projects that are currently in progress and are likely to leave behind extra "business as usual" costs after the project has completed.

Recast the landscape. Instead of working bottom up, a new design can be created more quickly by proposing a potential solution and then testing how it might work in the future. The new operating model might look very different, especially if an organisation is prepared to take brave, radical steps. On the other hand, the right answer for you might be a more modest approach that goes after the "low hanging fruit". Either way, there will be opportunities to eliminate work effort, combine functions, share components, and re-engineer processes.

Don't forget the hearts and minds. Not surprisingly, it is not easy to tackle risk and control convergence, and it can take time to put new solutions in place. Many people are surprised to hear that auditors and the other fauna to be found in the assurance world are people, not machines. They have their own fears and ambitions and agendas, and they will need to be taken to a new way of working. Like any transformation, this one needs to be communicated to stakeholders so they are properly engaged, and the transition needs to be carefully planned and managed. Quick wins can be helpful in generating early payback and momentum. But the best way to win over people is to unite them in a common goal that links assurance to achieving business objectives.



Independent Audit is at the forefront of assisting boards strengthen their strategic governance. As well as helping to improve board and committee performance, we provide advice on a range of issues such as internal control and assurance frameworks, control culture, enterprise risk management, risk appetite, and internal and external audit effectiveness.

If you would like to find out more about our services or discuss any of the ideas contained in this paper, please contact:

Malcolm McCaig
malcolm.mccaig@independentaudit.com
+44 (0)20 7220 6585

Jonathan Hayward
jonathan.hayward@independentaudit.com
+44 (0)20 7220 6582

Independent Audit Limited Holland House, 4 Bury Street, London EC3A 5AW

www.independentaudit.com