

Internal Audit: Planning – by James C Paterson

It has become commonplace to say we are now in an era of risk based auditing. It seems self evident that the work of Internal Audit (IA) should be focussed on the areas that matter the most. It also seems obvious that IA plans should be developed on a risk basis and obtain input from senior managers and the audit committee.

However, if you actually ask two Heads of Internal Audit (HIAs) to describe in detail the actual methodology that they use to come up with the IA plan, you find the methodology can differ quite significantly. Many of the differences reflect historical, cultural and practical differences between organisations, but over and above this are some key underlying questions it is worth exploring. Here are some of the key questions I have been exploring with my clients.

1. Do you mostly audit areas of known concern?

At one level it seems “obvious” to audit the areas management are concerned about. However, increasingly HIA’s are realising that whilst including these assignments in the plan can help IA seem “business focussed”, they can also increase the risk of IA being accused of not really coming up with anything that management didn’t already know about! In addition, such an approach will mean that areas of risk not yet identified by the organisation may continue to be unnoticed for longer, increasing the likelihood of a surprise from an unexpected direction.

There is a genuine dilemma at the heart of the question that can be illustrated by considering a leaking boat. Do you run over to the area of the leak and join in with the others – in the spirit of “all hands to the pump” to stop that leak from swamping the boat? Or might you judge that there are enough people already involved and start looking elsewhere around the boat for other leaks that may be going unnoticed?

Recommendation 1: HIAs should ask themselves: How much of the IA plan looks at known problem areas, and how much at i) emerging risk areas, or even ii) areas where it is commonly understood that everything is working well? Consider an IA management team discussion about the pros and cons of the current approach.

2. How often are you suggesting alternative sources of assurance?

Done well, the IA planning process should highlight gaps in risk management and risk assurance and opportunities for audit to demonstrate its value by looking at these areas and suggesting improvements. However, an increasing number of HIA’s are starting to wonder whether IA involvement should be the only response to a concern. For example, if there is a concern about how the organisation is addressing risks from 3rd party IT contractors, why not encourage the IT department to present what it is doing first, before any IA audit?

The use of direct assurances (whether in the form of a written paper or a presentation) can help emphasise the need for management to take accountability for risk management and risk assurance – an overarching objective that many HIA’s are realising is key to support a good risk and control culture in their organisation.

In addition, direct assurance discussions may help subsequent IA work to be more focussed – invaluable in an environment of resource constraints.

Recommendation 2: How often are direct assurance presentations or papers an outcome from the IA planning process? Consider suggesting direct assurances as part of the planning process – then do audits selectively if needed, based on what emerges from these up-dates.

3. And what about follow-up audits?

Another developing best practice centres around the role of IA should have in verifying whether or not findings have been fully remediated. There can be no doubt that IA needs to be aware whether its recommendations are actually being implemented, and equally it is understandable that IA will be asked to independently verify whether certain key risk areas have been closed off.

However, these objectives can be achieved by implementing an issue tracking process that can be used by staff and line management, as well as IA. Such an issue process or system can be used to capture all control issues in one place and also build the expectation that staff and management should be concerned about whether remediation is on track, and whether or not risk areas have been closed off satisfactorily. IA can then selectively review the highest risk areas for closure as judged appropriate by senior management and the audit committee.

In addition to freeing up resource in IA by a more selective approach to follow-ups, this approach has the important spin off benefit of stopping management from assuming that they don't have to concern themselves with how an issue has been closed, "since IA always checks its OK".

Recommendation 3: How much resource are you spending on follow-up audits? Look at the wording of your IA reports and check whether sufficient prominence is being given to management accountability for verifying issue closure? Think about implementing a issue tracking process or system that can be used by your whole organisation as well as IA.

4. Resource estimates in the plan: The importance of paying attention to the purpose of the audit and the use of alternative approaches such as reviews.

Suppose that an area has been identified to be on the IA plan. The resource estimate for such an audit might be informed by the time taken to review that risk or process in past years. Whilst this is an understandable approach it is easy for value to "leak" from such an assignment. My advice is that HIA's need to ask two key questions during the planning process:

1) Which areas of the process or risk are of most interest from an assurance perspective?

In relation to the earlier 3rd party IT contractor example: Is the concern about the overall process for 3rd party contracting or in relation to a specific supplier? In any event do the concerns that prompted an interest in having an audit relate to data privacy, or is the concern about value for money and the rigour of accounting underpinning cost recharges, or is the key concern about disaster recovery capabilities, or even a more general interest in compliance with service levels as specified in the contract?

It should be obvious that simply doing a general review of 3rd party IT contractor processes will use more resource than a more focussed review. Moreover, a general

review may not adequately probe the specific risk area that stimulated the request in the first place.

II) Would a high level review be acceptable at this stage, or is it expected that all risks and controls will be looked at in depth?

Many IA functions can recount examples of devoting many days of audit work looking at many risks and controls in detail, when it becomes clear from stakeholders later on that a high level review of key controls would have been sufficient. By way of example, is a high level assessment of privacy governance, policies and accountabilities going to be adequate, or also a walk through of the data privacy process in a specific area or would is detailed data checking of a specific class of transactions (or a broad sample of transactions) going to be needed. Hopefully it is self-evident how different the resource estimates for these different sorts of reviews or audits would be.

Recommendation 4.1: Seek to establish the key areas of risk or concern when risks or processes are identified for inclusion on the plan, and ensure the focus of IA's work is on these areas. Ensure areas of scope in the audit reflect these priorities.

Recommendation 4.2: If you are not already doing so, during the planning process, start asking "Would you like an in-depth audit of this area, or would a high level review of key controls be sufficient at this stage"?

5. At the end of the day, does the plan make sense top down?

Many IA plans are built up through scoring an audit universe against a number of criteria – risk ratings, past audit results, time since last audit etc. Whilst such an approach has its place, it is not uncommon to have a sense that only one or two of the IA team members fully understand how this works and furthermore, a lingering suspicion that, despite its complexity, the plan is not quite addressing all the areas it should be.

Recommendation 5: HIA's should employ a series of "top down sanity checks" of their draft IA plans to ensure that they are not missing "the wood for the trees".

Typically top down sanity checks will highlight blind spots in the detailed planning process (for example new projects, or areas of risk) and can challenge the IA function to limit the number of routine audits in the same area.

Some of the top-down sanity checks that can be employed are:

i) How many of the key risk areas of the organisation are being looked at in the plan and how many not? Note that a review or audit of a process that is relevant to a key risk is not the same as actually auditing the specific risk.

II) How many of the key external disclosures made by the organisation are being considered? This needs to include non-financial disclosures, not just financial disclosures.

III) How many of the key business improvement / change projects for the organisation are being looked at?

IV) What is the overall spread of IA time in the plan between Financial Controls, IS/IT controls, Operational controls, Change projects and key risks? What is the "cycle time" of coverage for each area?

In each area the presence of other sources of assurance may explain why an IA review is not needed, but a proactive use of such sanity checks should avoid major gaps.

6. Are the choices in the IA plan transparent, especially the implications around resource?

Clearly the presentation of the IA plan to senior management and the Audit Committee should give them a sense that the proposed IA plan should be supported. At the same time, this can lead HIA's to feel tempted not to highlight some of the difficult choices that might have need to have been made in order to arrive at the plan.

Recommendation 6: HIA's should be crystal-clear about the choices being made in the plan, particularly in relation to areas not being looked at or only being looked at a high level.

When there is clear transparency in the IA planning paper in relation to these issues it becomes much easier to have a mature conversation concerning resources. Thus when asked "Does IA have enough resource?", an HIA can respond: "Well on the basis you want me to look at 6 of the top 10 risks; 3 in depth and 3 at a high level – Yes. If you wanted IA to look at another 2 of the key risk areas, or review some risks in more detail, we would need additional resource. Alternatively we could organise some direct assurance for you".

Such an approach to resource issues in the plan allows for a more rigorous way of teasing out the implications of budgetary decisions for IA and can also encourage a more holistic approach to the use of other assurance processes and functions and the value for money they offer. Extending management attention from the cost of IA to the overall cost of assurance is something an increasing number of functions are realising is important in these cost constrained times and one of the reasons for the strong interest in assurance mapping techniques, which I am also extensively involved in with my clients.

If you would like to discuss any of the issues arising from the paper, including assurance mapping or lean auditing, please don't hesitate to get in contact.

James C Paterson

James the founder of Risk & Assurance Insights Ltd. and his website can be found at:
http://web.me.com/jcpaterson/Risk_&_Assurance_Insights_Ltd/Welcome.html

e-mail: jpaterson2@btinternet.com

Mobile: +44 (0)7802 868914