COMMERCE AND INDUSTRY

INTERNAL AUDIT ROUNDTABLE

1 INTRODUCTION

In Q3 2016, specialist finance, accountancy and advisory recruiter Marks Sattin hosted an Internal Audit Roundtable at the DoubleTree Hotel in Leeds.

The event brought together heads of internal audit and senior managers in internal audit and risk from a wide range of commercial and industrial organisations, including **Royal Mail, ASDA, Greencore, Morrisons, NISA, Costcutter** and **Jet2**, as well as directors from **KPMG** and **PwC**.

The 15 attendees discussed various aspects of *risk management*, the impact of *Brexit*, and approaches to the use of *data and IT auditing*. This white paper summarises the conversation.

2 RISK MANAGEMENT

An organisation's attitude towards risk is reflected in the degree to which risk is embedded across the business. This varies by degrees. One participant noted: "Risk management to us is compiling a risk register to drive our audit plan and that is literally it for now." Another said that in their organisation, risk management has become rooted across the business, with each department having both a risk register and a risk champion. This was described as risk management that is 'genuinely embedded' and which drives decisions and operational focus.

Risk management is never entirely separate from internal audit. One participant responded that in their organisation each business has its own risk management committee that is owned by the respective business. However, internal audit had provided the committee framework and sends a representative to attend every meeting.

Another participant said that their business had instituted risk management via a "long hard process over four or five years". "We've developed a process that is acceptable to the board and is spread right across the whole business, so it's a bottom-up approach, from site and functional level condensed down to divisional and group level for board and audit committee approval." Most of the organisation also now includes risk management in objectives, and features it in job descriptions. The participant concluded: "We are all about risk management now: identifying risks and understanding how to measure controls."

3 THE ROLE OF THE RISK REGISTER

Should risk registers drive the business or should the business drive the risk register? Several participants noted that their risk registers drive decision-making and work programmes in their business; or help play a useful role in communicating the importance of some risks. They can also be used to measure the financial impact of risks over time.

Another participant noted that an acid test is how dynamic the risk register is. "It shouldn't be static. Far from it," they said. "You should always be having active risk-based discussions about things like Brexit."

A range of mechanisms are used to gather different views of risk. One participant described collecting issues from external data on things like data security and supply chain, and combining this with insights from stakeholder meetings and input from the business's globally dispersed audit team. "Typically we find that there is a Venn diagram, if you like, of all those things that overlap. The interesting thing is finding the issues that are common to all of them."

Another participant mentioned using core financial controls as well as the risk register to identify audits. "Management have expressed a preference for us to cover core financial control stuff just to get assurance over that," the participant explained. "And you find that you tend not to have core financial controls on the risk register. Something like paying ghost employees isn't there because it's never going to bring down the company, but there is still an appetite to have assurance over that."

Someone else said they develop a risk universe through their planning process and in response to management requests. Also they proactively go into the business and ask, 'Is there anything going on in this project? Can we get involved?' It was noted that management requests can come from the parent company, in which case, "We want to know why it's important to them and weigh it up against the things that are important to us."

A different participant noted that auditors need to be careful about management requests, there's a risk that you are either being asked to do things they should do themselves, or that internal audit is seen as an extra investigative resource or a political tool: "They feel like they're not getting all the information out of finance, so you are asked to find it out for them."

4 WHAT GOOD RISK MANAGEMENT LOOKS LIKE

Good risk management is characterised by buy-in from the top of the organisation. The structure of the risk register is also important. "It should try and get quite quickly to what needs to be done next," it was explained, "What the key actions are for the next six months. You want to move things along rather than have too much documentation."

An amazing proportion of risk registers don't have action plans, so internal audit needs to issue guidance on how each risk register should be written. This is particularly helpful at the point when internal audit has to collate many registers together, to present a consolidated version to the board. Risk registers also need to score the impact of risks on the business; this drives the right level of risk mitigation. They should include tolerances and key indicators so that changes can be monitored. Consideration also has to be given to the fact that the risk appetite will likely vary across the business: "There's the highly regulated part of the business and the entrepreneurial part of the business."

The group identified that getting everyone in the business up to speed on risk management is also a challenge. "You talk about gross risk and net risk and target risk. But what does it mean to them? It's about trying to educate people across the business, particularly if you're starting with project and departmental risk registers."

Another participant added: "You have to make it real to the person doing the job. But if you go too granular, you get too many risks that aren't that important, you know, like running out of coffee!" A final challenge is getting the board to write down a risk appetite statement, because directors may not agree. Also boards sometime simply have to walk before they run. "In one of my presentations," noted one participant, "I said that we were not going to discuss risk appetite because you guys are nowhere near ready to have that conversation. It will probably be 18 months to two years after we've embedded risk management that we can we start on that. Sometimes you have to pick your battles."

5 THE IMPACT OF BREXIT

It was felt to be too early to do much about the impact of Brexit. One month after the vote, our roundtable attendees were mindful of its potential impacts but felt that detailed planning would be premature. The market impact was as yet unknown so a 'wait and see' approach prevailed. However the sectors with significant numbers of migrant workers were paying the most attention.

One participant noted that since, as internal auditors, they were always thinking about legislation, regulation and government interventions in some way, Brexit was just an extension of that. Meanwhile, operationally, there was nothing to do until the outcome of negotiations is known.

Another participant cautioned against doing too much planning and assessing. "Until we actually know what will happen, burning so much time on it, when in two years' time things will be exactly the same, is a waste."

Others were keeping an eye on key strategic areas, such as the supply chain and the impact on businesses that employ a significant proportion of EU nationals, even though employing immigrant workers is already burdensome, with visas, passports, rights to work and so on to be processed. In truth nobody yet knows if the end result will be massively different from now; and until we do, it is too soon to start recruiting, for instance.

One participant mentioned they were looking at the risk of a potential skills drain, and assessing the need to relocate financial services to another part of Europe. Another echoed concerns about negative scenarios around the movement of people. One last contributor said that they had been asked to write a Board paper on Brexit, "But in terms of internal audit, as yet there's nothing to do."

6 IT AND DATA

The roundtable's final discussion focused on IT and data: specifically how useful are data techniques to internal audit; the challenges of data techniques; and what was the best way for internal audit to resource IT audits?

7 DATA TECHNIQUES

Data techniques were not felt to be hugely helpful to today's internal auditors. One participant said that they had had 'a play with ACL' but weren't sure it was worth the effort. Another said they try not to repeat analysis that's being done elsewhere in the business: "We've got so much data and an enormous amount of people providing analysis and making decisions on the back of it, so I don't want to replicate what they do." Also they were more concerned with the security of data flows from their business to external suppliers.

A more interesting question is whether the business's data analysis teams get consistent results: in other words, what can it tell us about the integrity of the organisation's data? "We're asking them so we can go to the board and say: 'Yes we can give you assurance that we have a single version of the truth'." Data is being used much more to target operational risks by identifying triggers and anomalies. This might involve things like the use of continuous comparative monitoring between divisions.

Data is also a good way for internal audit to justify its existence. "An example is say purchasing. You can use data to show who buys what and then you can say: 'Well, you made 1,000 orders under £10 and you have volume-based discounts in your contracts, so if you collate those you will save X over Y." It is also increasingly difficult for internal audit to justify a big investment in data analysis in particular because it is largely moving away from answering 'black and white questions' and towards things that were less 'cut and dried' like cultural and talent audits.

In summary, the group felt that data techniques were less relevant to the strategic based, non-process type audits that they performed.

8 HOW TO RESOURCE IT AUDITS

Finally, whether audit functions should recruit IT auditors or outsource depends on value for money and utilisation. In the main, the group outsourced because the majority felt that it's just not cost effective to use a dedicated internal resource. One participant noted: "I have to ask what I'll get out of having an internal person. I'm really trying to understand in my own mind will they be fully utilised or will they just be playing Candy Crush a lot." As well, external resources may well add more value because they bring a wider perspective.

It's also a concern whether one internal IT auditor will be able to cover all requirements. "I think the challenge is you almost expect them to be all things to all people. You want them to do lots of, I don't know, script testing, something quite technical, or it could be that you want them to articulate the IT risk assessment and what the programme should be there. It is quite a big range for one person to do." Meanwhile some group members were using hybrid approaches, where organisations have a core team of IT auditors doing IT General Controls, for instance, and in addition, bring in specialist outsourcers to do something like a specific cyber review. It was felt that for big organisations, a hybrid approach can work well. Another possibility is hiring an IT auditor who can also do other types of auditing.

It was also possible for internal audit to tap into the expertise of a PCI Qualified Security Assessor. "If you get a good relationship with the qualified assessor, they can suggest quite pragmatic and sensible things for you to put in place that work really well for general IT security."

Finally, some participants said that they did need an internal resource because of the volume of work to be covered. One participant said: "A fair percentage of our audit plan next year will be looking at IT processes, so to have that internal resource will be important." In addition, they were careful to recruit the right IT resource. "Not someone deeply technical, but who can work with our teams."

At the end of the day, IT auditors are considered a valuable resource as long as you can provide them with enough work and identify the value they bring to the audit plan.